ELECTION COMMITTEE STRATEGIC PLAN

Chair: Secretary Connie Lawson | Co-Chair: Beth Dlug

September 2018

Indiana Executive Council on Cybersecurity

Election Committee Plan

Contents

Committee Members

Committee Members

Name	**Organization**	**Title**	**Committee/Workgroup Position**	**IECC Membership Type**
Connie Lawson	Secretary of State	Secretary of State	Chair	Voting
Beth Dlug	Allen County	Elections Director	Co-chair	Advisory
Seth Cooper	Baker Tilly	Project Manager	Full Time	Advisory
Brad King	Indiana Election Division	Co-Director	Full Time	Advisory
Angie Nussmeyer	Indiana Election Division	Co-Director	Full Time	Advisory
Laura Herzog	Hendricks County	Elections Supervisor	Full Time	Advisory
Jay Phelps	Bartholomew County	Clerk	Full Time	Advisory
Jay Bagga	Ball State University	Co-Director, VSTOP	Full Time	Advisory
Sean Fahey	GCR	Elections and Campaign Finance Director	Full Time	Advisory
Dave Sturgeon*	Tippecanoe County	CIO	Full Time	Advisory
Brandon Clifton	Secretary of State	Deputy Secretary of State	As Needed	Advisory
Valerie Warycha	Secretary of State	Director of Communications	As Needed	Advisory
Jerry Bonnet	Secretary of State	General Counsel	As Needed	Advisory
Thomas Vessely	Secretary of State	Director of IT	As Needed	Advisory
Patrick Glover	Secretary of State	Asst. Director of IT	As Needed	Advisory
Gerry Baliey	iLab LLC	Director	As-Needed	Advisory

*Resignation effective 6/30/2018

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Interaction with several leading election cybersecurity organizations and initiatives.
  - Intelligence and situational awareness - evaluation of information, experiences, perspectives and concerns from across the sector.
  - Identification and assessment of cybersecurity vulnerabilities - i.e. phishing exercises, cyber hygiene assessments, and election system physical security and logical security controls.[1]
  - Identification and assessment of election cybersecurity authoritative information and best practices.

- **Research Findings**
  - Major election systems (voting systems, electronic poll books and associated equipment, software, and documentation) cybersecurity concerns center on Statewide Voter Registration Systems (SVRS), voting equipment physical and logical security controls, and network security.
  - Election cybersecurity involves systems and processes in use before, during, and after Election Day, including:
    - network user training and access authentication
    - physical security and cybersecurity of election systems
    - training for election officials, administrators and poll workers
    - network monitoring
    - election system certification and testing
    - election system physical and logical security controls
    - voting, tabulation, results reporting, post-election risk limiting audits
    - incident response and public communications
  - Election cybersecurity also encompasses networking with national and state security agencies and sector coordinating councils, training, incident response planning, and public awareness.

- **Committee Deliverables**
  - Statewide Voter Registration System (SVRS) Cybersecurity Enhancement
  - SVRS Network User Access Control Enhancement
  - Election System Physical and Logical Security Controls Assessments and Guides
  - Post-Election Risk Limiting Audit Standards and Pilot Program (included in the deliverable “Indiana Best Practices Manual for Operation of Election Equipment” below).
  - Cyber Threat Awareness and Training for County Election Administrators
  - Election Day Cybersecurity Tabletop Exercises
  - Indiana Best Practices Manual for the Operation of Election Equipment
  - Election Day Cybersecurity Emergency Preparedness Plans
  - Election Day Cybersecurity Monitoring and Rapid Response Technical Support

[1] Logical Security consists of software safeguards for an organization’s systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network. It is a subset of computer security.

  - Election Cybersecurity Public Education and Awareness
  - Election Cybersecurity Incident Response and Communications.
  - Catalog and Summaries of Best Election Cybersecurity Reports and Guides.

- **Additional Notes & References**
  - Notwithstanding heightened concerns resulting from the discovery of foreign attempts to penetrate voter registration systems prior to the 2016 General Election, election security and cybersecurity are not new issues in the realm of election administration. As of mid-2018 the election cybersecurity environment remains dynamic and of continuing public concern.
  - The Secretary of State and Indiana Election Division have been, and continue to work, closely with U.S. Department of Homeland Security (USDHS), the Election Infrastructure Multi-State Information Sharing Analysis Center (MS-ISAC), the National Association of Secretaries of State (NASS) Election Cybersecurity Task Force, the Indiana Department of Homeland Security (IDHS) and Indiana National Guard (INNG), the Voting System Technical Oversight Program at Ball State University (VSTOP) and other government, academic, and industry resources.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   a. Well before the 2016 Election cycle, which gave rise to the national push for election cybersecurity. Indiana was aware and preparing to respond to the threat. In 2014 and 2015, the Secretary of State and the Indiana Election Division identified the need for Statewide Voter Registration System (SVRS) modernization and IT security enhancements. In furtherance of those priorities, Indiana developed a modernization roadmap and budget proposal, which was authorized and fully funded by the Indiana General Assembly in 2017.
   b. Training on security concepts for county IT support; information from vendors regarding best practices; phishing exercises for county election staff; continual training and awareness for county election officials, administrators and poll workers.
   c. Received and responded to national security agencies, industry, and association intelligence gathering and situational awareness. Participated in national and state forums for information gathering, exchange, analysis, and response coordination.
   d. Engaged cybersecurity assessment programs provided by USDHS and commercial vendors.
   e. Electronic poll book vendors have been surveyed regarding cybersecurity best practices. The survey included questions regarding server set up, security processes for election activity (including third-party servers on the cloud), backup and fail-safe data recovery procedures, file naming and versioning procedures and existence/maintenance of a security breach emergency crisis plan in the event there is unauthorized access to data and/or equipment. The results of this survey have been used to compile a list of best practices for cybersecurity of electronic poll books. Note: a similar survey is planned for election system vendors.
   f. VSTOP prepared the *Indiana Best Practices Manual for the Operation of Election Equipment.* The manual includes best practices for cybersecurity. Copies of the manual have been distributed to Election Officials in all 92 counties in Indiana.
   g. VSTOP organized the first post-election risk limiting audit (RLA) in Marion County which was also the first audit anywhere which used the Bayesian RLA method. Report submitted to the Indiana Secretary of State in August 2018.
   h. VSTOP has developed and recently launched an advanced professional election administrator certificate program, including specific cybersecurity training. The program's first class began in August 2018. The Secretary of State's office has provided scholarships for the first 16 students enrolled in the program.
   i. Election system and electronic poll book vendors with equipment used in Indiana elections are required to monitor and record performance anomalies. Performance anomalies are required to be reported to VSTOP for investigation and analysis as warranted and reported to the Secretary of State and Indiana Election Division.
   j. Legislation directed at election system physical security was enacted and implementation has begun.
   k. The Secretary of State and Election Division have initiated pre-election and Election Day emergency preparations and planning, including cyber events and coordination with national, state and local security and emergency response agencies.

l. The Secretary of State and National Association of Secretaries of State lobbied Congress for expedited approval of $380 million previously authorized, but un-released, Help America Vote Act funds approved in March 2018 for election security. Indiana applied for and received approval for approximately $7.6 million funding, approved in July 2018, and initiated planning for county sub-grants, SVRS upgrades, and cybersecurity initiatives. As a result of the State's proactive election cybersecurity initiatives, Indiana expects to have met its 5% federal grant match obligation.

m. VSTOP was among the founding institutions of the annual State Certification Testing of Voting Systems National Conference. The academic conference established in 2011 focuses on election security (http://bowencenterforpublicaffairs.org/institutes/policy-research/election-admin/conference). This conference was held in Indianapolis in 2012.

n. The Secretary of State and Election Division will be participating in an election cybersecurity session at the upcoming Cybertech Midwest Conference (October 2018, Indianapolis, Indiana).

2. What (or who) are the most significant cyber vulnerabilities in your area?

a. Malicious cyber hacking and unauthorized access to voter registration system data; particularly initiated by a sophisticated domestic or overseas perpetrator.

b. Cyberattacks aimed at: political parties, campaigns and candidates; the voter registration database system and user network; electronic poll books; election systems; and election result reporting systems managed by state and county election officials.

c. Malicious, anonymous, false or misleading social media activity aimed at political parties, campaigns and candidates.

d. Identifying cyberattacks or other election interference.

e. The voting systems physical security (addressed by SEA 327-2018), and election system logical security (addressed by certification standards, testing, monitoring and post-election risk-limiting audits).

f. Lack of network user and public awareness of cybersecurity principles and threats (addressed by communications, training, and uniform adherence to security protocols and best practices).

g. Any unaddressed actual or perceived cyber threat that adversely affects voter confidence.

3. What is your area's greatest cybersecurity need and/or gap?

a. Sophisticated cyber threat intelligence gathering, monitoring, and response as provided by national security agencies, sector coordinating councils and specialized vendors.

b. Identifying the presence of undesirable voting system cyber risk events and a process to assess the impact on counties, vendors and the State.

c. Identifying, verifying and implementing best cybersecurity practices for election systems, networks, election officials, administrators and poll workers.

d. Identifying, verifying and implementing best practices for election system physical and logical security.

e. Control or mitigation of false or misleading social media activity aimed at election interference.
f. Development of coordinated cyber incident communications and response.
g. Public awareness and communications.

4. What federal, state, or local cyber regulations is your area beholden to currently?

a. Federal and State election laws and administrative regulations (i.e. National Voting Rights Act, National Voter Registration Act, Help America Vote Act, Indiana Election Code).
b. Election system certification rules and protocols promulgated and administered by the Indiana Election Commission and Election Assistance Commission.
c. Indiana testing and certification requirements for election systems and electronic poll books.
d. Indiana Office of Technology cybersecurity standards and requirements for state agencies.
e. County policies and resolutions including cybersecurity protocols adopted by County Election Boards.

5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?

a. Handbook for Elections Infrastructure Security – Center for Internet Security.
b. The State and Local Election Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
c. Campaign Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
d. Election Cyber Incident Communications Coordination Guide – Harvard Belfer Center.
e. Elections Security Checklist - National Association of Elections Officials Election Center.
f. SEA 327-2018 Voting System Security – Indiana Election Division Presentation.
g. Indiana Best Practices Manual for the Operation of Election Equipment - Voting System Technical Oversight Program at Ball State University.
h. Post-Election Risk Limiting Audit Pilot, Marion County Indiana, May 2018 - Voting System Technical Oversight Program at Ball State University.
i. Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; report submitted to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.
j. US Elections System as Critical Infrastructure – Addendum I: Glossary of Key Terms and Acronyms - U.S. Election Assistance Commission.
k. NASS Election Cybersecurity Task Force Survey – National Association of Secretaries of State.
l. ISAC Pilot for Election Infrastructure – DHS/EI-ISAC.
m. Glossary of Common Cybersecurity Terms – U.S. Election Assistance Commission.
n. Common Cyber Security Language – U.S. DHS National Cybersecurity and Communications Integration Center (NCCIC).
o. National Conference of State Legislatures Election Security: State Policies: http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
   a. Handbook for Elections Infrastructure Security – Center for Internet Security.
   b. The State and Local Election Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
   c. Campaign Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
   d. Election Cyber Incident Communications Coordination Guide – Harvard Belfer Center.
   e. Elections Security Checklist - National Association of Elections Officials Election Center.
   f. SEA 327-2018 Voting System Security – Indiana Election Division Presentation.
   g. Indiana Best Practices Manual for the Operation of Election Equipment - Voting System Technical Oversight Program at Ball State University.
   h. Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; report submitted to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.
   i. US Elections System as Critical Infrastructure – Addendum I: Glossary of Key Terms and Acronyms - U.S. Election Assistance Commission.
   j. NASS Election Cybersecurity Task Force Survey – National Association of Secretaries of State.
   k. ISAC Pilot for Election Infrastructure – DHS/EI-ISAC.
   l. Glossary of Common Cybersecurity Terms – U.S. Election Assistance Commission.
   m. Common Cyber Security Language – U.S. DHS National Cybersecurity and Communications Integration Center (NCCIC).

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
   a. The National Association of Election Officials Election Center has promulgated and distributed an Elections Security Checklist.
   b. The Harvard Belfer Center and USDHS have developed and are presenting Election Tabletop Exercises to election officials and administrators.
   c. The National Association of Secretaries of State Election Cybersecurity Task Force surveyed states on election cybersecurity practices.
   d. The US Election Assistance Commission has posted materials, documents and videos, related to elections cybersecurity.
   e. The National Conference of State Legislators and California have created cybersecurity task forces.
   f. The National Association of Secretaries of State is tracking federal election security initiatives and the National Council of State Legislators is tracking state election security legislation.
   g. The annual State Certification Testing of Voting Systems National Conference focuses on elections security. (see: http://bowencenterforpublicaffairs.org/institutes/policy-research/election-admin/conference/raleigh-conference-2018/%20raleigh-conference-2018-agenda)
   h. Colorado and Wisconsin have developed extensive cybersecurity training programs for local election administrators.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Year One – priority programs developed; Year Three- deliverables developed with training programs; Year Five – no successful penetration of election systems or databases essential to conducting elections.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Indiana's county election officials and administrators need cybersecurity communications training to promptly and accurately inform the public regarding the safety and security of the systems and to respond to cybersecurity incidents in an appropriate and coordinated fashion.
    b. A statewide public awareness campaign is being developed and will be launched in time for the November 2018 General Election.
    c. VSTOP has developed and launched an advanced professional election administrator certificate program. The program's first class began in August 2018. The Secretary of State's office has provided scholarships for the first 16 students enrolled in the program.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. In addition to the Secretary of State's office and Election Division, every Indiana county has election workforce including officials, administrators and poll workers. The IT and cybersecurity workforce within each county varies according to population, resources and other factors.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A trained, ready workforce should attract cyber companies. Programs at Indiana's universities, colleges and technical schools providing state of the art training for the IT and cybersecurity workforce should be supported.
    b. Indiana can continue to host leading cybersecurity conferences such as the Cybertech Midwest Conference.
    c. State agencies can gather information regarding potential cybersecurity service vendors and issue a public request for proposals (RFP)/request for quotations (RFQ)/Quantity Purchase Agreement (QPAs) for cybersecurity assessments and initiatives after needs and priorities have been identified.

12. **What are your communication protocols in a cyber emergency?**
    a. Under Indiana law, a cyber incident that could impact election administration is to be immediately reported to the Secretary of State.
    b. The Secretary will communicate the details of the incident to appropriate responding security and intelligence agencies and Election Division.
    c. The Election Division will communicate with county election officials and administrators, state agencies, vendors, association and industry partners as appropriate.
    d. The Secretary of State will coordinate public communications through media channels as warranted.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Cybersecurity awareness training, communication, risk assessment and risk mediation for state agencies, employees and IT vendors.
    b. Ongoing cybersecurity awareness training for all Hoosiers.

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

General Information

1. **What is the deliverable?**
   a. Enhanced Statewide Voter Registration System (SVRS) cybersecurity though installation and operation of additional critical protections to prevent and detect unauthorized intrusion.

2. **What is the status of this deliverable?**
   a. 100% complete

3. **Which of the following IECC goals does this deliverable meet?**

☐ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

☐ Research – Surveys, Datasets, Whitepapers, etc.
☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Secure the State’s voter registration database system with state-of-the-art protections in coordination with agency partners.

6. **What metric or measurement will be used to define success?**
   a. Prevention of unauthorized access to SVRS.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. The State as custodian and administrator of the SVRS, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State resources were used to implement these enhancements.
    b. Some portion of Federal Help America Vote Act (HAVA) funds released to Indiana in 2018 may be allocated to maintenance of these enhancements.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Indiana Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Maintaining the highest level of security for the SVRS will be an ongoing and likely evolving effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Protocol Utilization	SOS Exec. Staff	100%	N/A	
Implement Critical Protections	SOS IT Staff	100%	N/A	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes – see below:

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1-2 hrs	N/A	Technical	State	HAVA	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Enabling critical protections to improve the security posture of our elections network.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Having these critical protections provides an additional layer of security making it less likely for any threat to successfully infiltrate the network.

19. What is the risk or cost of not completing this deliverable?

a. One less layer of security.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success can be measured by the data/metrics generated from these efforts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Given this effort requires support from a third party vendor. Delays in anticipated completion and service disruptions are possible.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Certain protections will require maintenance.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Statewide Voter Registration System Core Team.

27. Can this deliverable be used by other sectors?

a. No – due to unique system functions and characteristics.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators are aware of the SVRS security enhancements.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes – to the extent required by the Indiana Open Door and Public Records Acts.

30. What are other public relations and/or marketing considerations to be noted?

a. None – SVRS security protocols and enhancements are not public facing.

Evaluation Methodology

Objective 1: Indiana Secretary of State Office will begin utilizing additional security protocols in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Statewide Voter Registration System (SVRS) Network User Access Control Enhancement

Deliverable: SVRS Network User Access Control Enhancement

General Information

1. **What is the deliverable?**
   a. Statewide Voter Registration System (SVRS) network user access security upgrades.

2. **What is the status of this deliverable?**
   a. Indiana's first statewide voter registration system successfully began operating in all 92 counties in December 2005, making Indiana one of the states to achieve the 2006 implementation deadline for SVRS set by the federal HAVA law. During the two years before this rollout, the State worked with skilled system designers to ensure that SVRS included numerous safeguards to prevent the deliberate or accidental corruption of voter registration data. In the years following the 2005 rollout, Indiana continued to learn from both SVRS county system users and from the experience of other states to identify and implement additional enhancements to prevent intrusions into the system. The existing SVRS system has a robust framework to safeguard voter registration data.
   b. Even before heightened national awareness of cybersecurity issues during and after the 2016 election, Indiana had begun studying and implementing innovative features to further improve SVRS security. With the assistance of specialized vendors and project managers, technology and protocols for SVRS user access security upgrades were specified and successfully tested with strategically selected user groups. The user access upgrade pilot program is 100% complete. Implementation of multi-factor authentication have commenced. All users will utilize multi-factor authentication or token for the November 2018 General Election.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Implementation of state-of-the-art user access controls including multi-factor authentication tools.

6. **What metric or measurement will be used to define success?**
   a. Implementation of security upgrades, metrics from ongoing monitoring.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
   a. State as custodian and administrator of the SVRS, system users, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. State resources were used to implement these enhancements.
   b. Some portion of Federal Help America Vote Act (HAVA) funds released to Indiana in 2018 may be allocated to maintenance of these enhancements.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Indiana Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Multi-Factor Authentication	SOS Office and Indiana Election Division	100%	December 2017	
Multi-Factor Authentication	SOS Office and Indiana Election Division	100%	December 2017	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Multi-Factor Authentication.	The physical token is required for participating pilot counties to access SVRS.	$100,000.	N/A	State	HAVA	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. New authentication features were added to the Statewide Voter Registration System (SVRS) to increase the security of the system.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Counties participating in the pilot will reduce their cybersecurity risk since multi-factor authentication expands the validation protocol.

b. Because most attacks are targeted during after-hours (in an effort to prevent detection), an additional validation tactic will be required for users attempting to access SVRS during those after-hours.

19. What is the risk or cost of not completing this deliverable?

a. Not completing these deliverables inscreases risk that an attacker might gain access to SVRS. It is a method of confirming a user's claimed identity by utilizing a combination of multiple factors of authentication.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. A key success objective includes reducing cybersecurity threats and maintaining needed functionality in SVRS. User Acceptance Testing (UAT) validates that the software functionality meets the requirements in real-world scenarios and is a key systematic metric used to measure success. Users are able to provide enhancement suggestions at any time, which help evolve the functionality on an ongoing basis. Specific to the pilot, every six weeks' feedback is collected and evaluated from participating county users to identify and resolve issues, and will be used to evaluate the pilot success for consideration of a statewide rollout.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes.
    b. Many states are inquiring about similar projects used in Indiana. New Jersey, Colorado, and West Virginia are believed to have similar projects completed or in-progress.

22. **Are there comparable jurisdictions (e.g. other states) that do not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes.
    b. Arizona did not use a comparable project in the 2016 General Election, and a county user experienced an intrusion.Arizona did not use a comparable project in the 2016 General Election, and a county user experienced an intrusion.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. This is not applicable since deliverables were completed within the agreed upon timeline and budget.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No.

25. **What will it take to support this effort if it requires ongoing sustainability?**
    a. The Indiana Secretary of State, Indiana Election Division, 92 county election officials, and vendor partners will continue to evaluate best practices and, as situations warrant, enhance security capabilities as needed. The Indiana Elections Cybersecurity Council does not need to set aside resources for assistance.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. All 92 county election officials are aware of the implementation of these deliverables.

27. Can this deliverable be used by other sectors?

a. Yes.
b. All other sectors looking to implement multi-factor authentication needed for user access to sensitive or private data.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. The Indiana Secretary of State, Indiana Election Division, and all 92 SVRS users.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes – to the extent required by the Indiana Open Door and Public Records Acts.

30. What are other public relations and/or marketing considerations to be noted?

a. Development of messaging for the public without divulging any confidential information, which could compromise security.

Evaluation Methodology

Objective 1: SOS Office and Indiana Election Division will implement the Statewide Voter Registration System (SVRS) user access/authentication upgrades with one-hundred percent of counties by January 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 2: SOS Office and Indiana Election Division will launch a Two-Factor Authentication Token Pilot by March 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: SOS Office and Indiana Election Division will provide a report on Two-Factor Authentication Token Pilot by May 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election System Physical and Logical Security Controls

Deliverable: Election System Physical and Logical Security Controls

General Information

1. **What is the deliverable?**
   a. Best practices for voting system logical and physical security. This deliverable is included in the deliverable "Indiana Best Practices Manual for Operation of Election Equipment."

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Best practices guidelines for protecting, testing and storing voting systems.

6. **What metric or measurement will be used to define success?**
   a. Availability and acceptance and use of guidelines. Incorporation of guidelines into statutory requirements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
   a. State and County election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The Indiana Voting System Technical Oversight Program at Ball State University (VSTOP).

12. **Who should be main lead of this deliverable?**
    a. The Indiana Voting System Technical Oversight Program at Ball State University (VSTOP).

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Education on the Physical and Cyber Security Requirements in Election Codes	VSTOP	100%	July 2018	This is also tied to deliverable no. 7, which includes a best practices manual on the operation of election equipment
New Security Features in SEA 327/Public Law 100 (2018)	VSTOP	100%	July 2018	
Continued Encouragement of Legislation that Promotes Physical and Cyber Security of Elections	VSTOP		On-going	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Increased education and awareness of physical and cybersecurity best practices among election officials at the county and State level.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help train election officials to efficiently manage security risks. The estimated costs are unknown, for instance Public Law 100 (2018) allows counties to request funding assistance for certain security measures.

19. What is the risk or cost of not completing this deliverable?

a. Election process will be more vulnerable to physical and cybersecurity risks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. That the County Election Officials are able to successfully implement the requirements of the law and the best practices as specified in the deliverable.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes.

b. VSTOP will supplement after consultation with Election Assistance Commission (EAC)

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No. VSTOP will supplement after consultation with EAC. VSTOP will supplement after consultation with EAC.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None at this time

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Experience gained from implementing this deliverable could lead to recommendations of further revisions or additions to the Indiana Election Code.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. VSTOP has consulted various sources, such as the websites of the EAC, Election Center, National Conference of State Legislatures (NCSL) and Belfer Center at Harvard University.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State Office, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and Election Officials.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that Indiana takes great care and trains Election Officials in the best practices in physical and cybersecurity. In addition, publicity regarding the best practices being followed, as well as required, also provides assurance to voters and jurisdictions holding elections.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program will develop and distribute the Best Practices for Voting System Logical and Physical Security Manual to all Indiana counties in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program

Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program

General Information

1. **What is the deliverable?**
   a. Post-election risk limiting audit standards and pilot program.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Availability and implementation of a validated post-election risk limiting audit procedure.

6. **What metric or measurement will be used to define success?**
   a. Statistical confidence measures as well as general public confidence in election outcomes.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and county election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. The US Election Assistance Commission (EAC) provided expertise and assisted in the completion of this deliverable.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The US Election Assistance Commission (EAC).

12. **Who should be main lead of this deliverable?**
    a. The Voting System Technical Oversight Program at Ball State University.

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of pilot counties in Indiana where this deliverable can be tested.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort depending on determination of pilot RLA.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Research and Planning of RLA	VSTOP	100%	May 2018	Election Assistance Commission (EAC) is also assisting
Pilot RLA in Marion County	VSTOP	100%	June 2018	Pilot conducted May 2018.
Presentation on RLA Pilot at National State Certification Conference in Raleigh, NC	VSTOP	100%	June 2018	SOS approval received.
Post-Audit Analysis	VSTOP, Marion County & EAC (Jerome Lovato)	100%	August 2018	Report prepared.
Observation of Denver County RLA for Primary 2018	VSTOP Team Member	100%	August 2018	Report in preparation.
Pilot in Three Michigan Counties December 2018	Michigan	10%	January 2019	Draft Pilot Proposal/Plan in Progress; VSTOP is assisting the State of Michigan.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

b. At this time for the Pilot RLA's, VSTOP Team members, County Election Officials, and EAC will contribute their time. If RLA's are adopted and instituted in Indiana in all counties, using an optical scan voting system as its primary voting system, funding for an FTE or ½ FTE and/or resources may be required.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. **What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)**
    a. Post-election audits are gaining increasing acceptance across the country and are required by law in some states. Performing RLA results in increased confidence in election results.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. If Risk Limiting Audits are deemed successful and used in the future it could increase assurances in the election tallying process, which could then lessen the number of recounts and election contests that occur in counties using optical scan voting systems as its primary voting system.

19. **What is the risk or cost of not completing this deliverable?**
    a. If Indiana does not move forward in election security best practices, this can lead to a decrease in voter confidence in election results.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. The timely completion of an RLA for one county-wide race in the 2016 General and 2018 Primary Marion County elections. Ideally, we would like to complete three different audit methods: Comparison, Ballot-Polling, and the Bayesian Audit.
    b. Increased statistical confidence measures.
    c. Increased overall public confidence in elections and certain types of voting systems.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes.
    b. Arapahoe County, Colorado instituted a pilot RLA in one County prior to instituting it in all counties, that we can use for comparison. In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Others may be added after consultation with EAC.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes.
    b. Although many states, such as Colorado, Rhode Island, and Virginia require RLAs, most states do not.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The 2018 Primary absentee voting and preparations for Election Day resulted in the County staff, as well as the VSTOP and EAC team, assisting with the audit not being available until mid-May for the pilot.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes.

b. Currently, RLAs are not required in Indiana. If the pilot is deemed successful, Indiana may want to pursue legislation mandating their requirement in counties using optical scan voting systems as its primary voting system. Fiscal impact could include new costs, such as training, personnel and software.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. If RLAs were implemented in some or all of the 92 counties, then training, additional processes and forms, personnel, and potentially new software would be required.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. VSTOP has contacted Jerome Lovato Certification Program Specialist from the EAC, Dr. Ron Rivest of the Caltech/MIT Voting Technology Project, the Indiana Election Division Co-Directors, as well as the Marion County Election Director and Deputy Director.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State Office, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and Election Officials. See Supporting Documentation: Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; Report to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that risk limiting audits are being looked into in the State since many other jurisdictions outside of Indiana are conducting them already. In addition, publicity regarding the successful completion of RLA can provide additional assurance to voters in counties using optical scan voting systems as its primary voting system that the results of an election are accurate.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop and implement an RLA pilot in Marion County by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana Voting System Technical Oversight Program (VSTOP) will provide a report by August 2018 on the July 2018 RLA pilot in Marion County.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

General Information

1. **What is the deliverable?**
    a. Election cyber threat exercises and training for county election units (e.g. phishing exercises).

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Increased situational awareness of the cyber threat environment and implementation of cybersecurity best practices at the election county unit level.

6. **What metric or measurement will be used to define success?**
    a. Metrics from phishing exercises, surveys, and other assessments.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State, Election Division and County Election Officials.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Create initial phishing exercise	SOS IT Staff	100%		
Deliver on-going training & awareness	SOS IT Staff	Ongoing		Content has been queued and will be delivered beginning April 2018

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No.

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

   a. Continued education and awareness to the staff of potential threats to physical and logical security.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

   a. It will raise awareness and staff will be more vigilant with data sharing practices. No associated costs.

19. What is the risk or cost of not completing this deliverable?

   a. The risk is having staff unaware or uninformed, creating the potential for data leaks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

   a. The baseline has been set with the initial phishing campaign. Success will be measured by increased participation in training programs and decreased response to phishing attempts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

   a. No.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

   a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

   a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

   a. None.

25. What will it take to support this deliverable if it requires ongoing sustainability?

   a. Ongoing coordination with counties to effectively conduct phishing campaigns.

26. Who has the committee/working group contacted regarding implementing this deliverable?

   a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?

   a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

   a. Secretary of State and Indiana Election Division.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

   a. No.

30. What are other public relations and/or marketing considerations to be noted?

   a. None.

Evaluation Methodology

Objective 1: Indiana Secretary of State will implement and deliver a multi-year cybersecurity public awareness plan beginning in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eighty percent of Indiana election officials participate in state-offered training by November 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 3: See a thirty-percent decrease in click-through rates of Indiana election officials in State phishing campaign by April 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Tabletop Exercises

Deliverable: Election Day Cybersecurity Tabletop Exercises

General Information

1. **What is the deliverable?**
   a. Election security tabletop exercise program for state and local election officials and administrators.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Develop and deliver a training exercise program for election officials and administrators.

6. **What metric or measurement will be used to define success?**
   a. Availability of the program for county election administrator use during the 2018 Election cycle.

7. **What year will the deliverable be completed?**
   a. 2018 and 2019.

8. **Who or what entities will benefit from the deliverable?**
   a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana National Guard may be utilized for a complete exercise in 2019.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Deliver tabletop exercises to counties on how to conduct elections	SOS Staff	25%	April 2019	

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. Yes.

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
0.5	0.25	Skilled	Agency	N/A	

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. Election day equipment, exercise facilities.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit is providing consistent information to counties on conducting elections as well as awareness of potential threats or risks and methods for responding to them.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. The risk is reduced by increased training and execution of best practices.

19. What is the risk or cost of not completing this deliverable?

a. The risk is exposure of processes and information intended only for county election officials.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The baseline has yet to be established. The format for the tabletop exercises is being built off a model developed by the Belfer Center at Harvard.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Wisconsin.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of county election administrators to participate (timeline constraint).

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Commitment to participation at the county level.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State and Election Division.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Indiana Secretary of State will develop and deliver a training exercise program for election officials and administrators by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will conduct a tabletop election exercise by April 2019.
Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

General Information

1. **What is the deliverable?**
   a. Best Practices Manual for the Operation of Election Equipment.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Best practices Manual for Indiana election officials and administrators provides the most up-to-date considered best practices, promotes situational awareness and operational uniformity.

6. **What metric or measurement will be used to define success?**
   a. Completion and distribution of the manual for use in the 2018 General Election.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. U.S. Election Assistance Commission.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Indiana Secretary of State Office (SOS) and Indiana Election Division (IED).

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Secretary of State Office (SOS) and Indiana Election Division (IED).

12. **Who should be main lead of this deliverable?**
    a. The Indiana Voting System Technical Oversight Program (VSTOP) at Ball State University.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Workshops on Material in the Manual at Southern & Northern District Clerk Conferences in Early March	VSTOP	100%	March 2018	
Research and Construction of the Manual	VSTOP	100%	March 2018	
Submit Draft to IED/SOS for approval and feedback	VSTOP	100%	June 2018	
Submit Draft to Counties for review and feedback	VSTOP	100%	June 2018	Sent to all 92 Counties in June 2018 and asked for comments.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Increased education and awareness of best practices for the operation of election equipment, including physical and cybersecurity of elections, among election officials at the county and State level.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help train election officials in efficient management of security risks.

b. At this time, we are not aware of any additional associated costs with production of a best practices manual that will not be absorbed through VSTOP’s current budget. However, if the counties implement some of these best practices there may be new costs that are unknown at this time.

19. **What is the risk or cost of not completing this deliverable?**
    a. Lack of knowledge regarding the best practices that are a part of Indiana Election Code, as well as some possible security risks not being properly managed.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Completion and distribution of a manual, as well as positive feedback and implementation of the best practices at the County level.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes. VSTOP consulted materials on the EAC website and Belfer Center resources.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. None known to VSTOP.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. None.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. Ongoing monitoring and updating of evolving best practices.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. VSTOP has consulted various sources, such as the websites of the EAC, Election Center, National Conference of State Legislatures (NCSL) and Belfer Center at Harvard University.

27. **Can this deliverable be used by other sectors?**
    a. No.

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. Secretary of State, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and election administrators in all 92 counties.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that Indiana takes great care and trains Election Officials in the best practices in physical and cybersecurity. In addition, publicity regarding the best practices being followed, as well as required, also provides assurance and confidence to voters and jurisdictions holding elections.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop the Indiana Best Practices Manual for the Operation of Election Equipment by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

General Information

1. **What is the deliverable?**
    a. Election Day cyber incident and emergency preparedness plans for State and County election officials and administrators.

2. **What is the status of this deliverable?**
    a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Update existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to 2018 May Primary Election and future elections.

6. **What metric or measurement will be used to define success?**
    a. Completion and distribution of plans prior to the 2018 May Primary Election. Obtain feedback after the May election to update plans prior to the 2018 November General Election.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Service, Energy, Emergency Services, Pre to Post Incident, Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Plans for Indiana state and county election administrators	Secretary of State, Indiana Election Division	100%	April 2018	Working on cybersecurity incident updates.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
40	N/A	Admin.	Admin	Elections	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Up to date emergency preparedness plans for election officials, administrators and poll workers for the 2018 May Primary and November General Election.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Election officials, administrators and poll workers will have appropriate contacts for rapid assistance with emergency situations as well as procedural and legal guidelines for election disruptions.

19. What is the risk or cost of not completing this deliverable?

a. Risk of a significant or prolonged election disruption due to lack of preparation and delayed response. Delayed response increases the cost, time and complexity of correcting election interference. Disruptions and delays decrease public satisfaction and confidence in election outcomes.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. First, completing and distributing plans prior to the 2018 Primary Election. Second, usefulness of the plans in the event of an election disrupting emergency. Third, feedback from election officials, administrators and poll workers.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of administrative resources, intervening emergencies, new contingencies, or changes in situational status.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Continually updating plans as needed, particularly prior to elections, as conditions and events warrant.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The Indiana Election Division, emergency responders, and IT technical support resources.

27. Can this deliverable be used by other sectors?

a. Yes, but only to a degree. Generally, any government service provider could likely benefit from emergency and contingency plans. Election administration is a somewhat unique and specialized government service; therefore, the plans would need to be adapted to different sectors and activities.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State and county election officials and administrators along with emergency responders.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. The general public should be generally aware of the existence of emergency and contingency planning.

Evaluation Methodology

Objective 1: Indiana Secretary of State and Election Division will provide existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to May 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

General Information

1. **What is the deliverable?**
   a. Election Day cybersecurity technical support program and resources.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Cybersecurity technical support and resources (teams) to support State and local election officials and administrators.

6. **What metric or measurement will be used to define success?**
   a. Availability of adequate level of oriented and prepared cybersecurity technical support resources. Effective response to cybersecurity issues during 2018 May and November Elections.

7. **What year will the deliverable be completed?**

   a. 2018

8. **Who or what entities will benefit from the deliverable?**
   a. State and County election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. U.S. and Indiana Departments of Homeland Security.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Service, Emergency Services, Pre/Post Incident, Local Government, Strategic Resource.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Secretary of State, Election Division, Indiana Office of Technology (IOT), Indiana Information Sharing and Analysis Center (IN-ISAC), DHS, IDHS, MS-ISAC, IECC, local units.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Staff election IT/cybersecurity support call center on Election Day – with access to an assembly of technical resources for May Primary and November General Elections.	Secretary of State/Election Division	100%	April 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes (if Yes, please complete the following).

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2-3	0	General IT	Agency	N/A	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Availability of an oriented, well connected emergency resource to assist, troubleshoot, and resolve Election Day IT or cybersecurity issues. Will help secure the election and assure the public.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. IT issues can be assessed and addressed quickly with real-time communications from cyber network monitoring sources. Cyber alerts can be quickly disseminated throughout the Election Day sector.

19. What is the risk or cost of not completing this deliverable?

a. Unaddressed IT or cybersecurity issues could hamper the elections and negatively impact public confidence.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Numbers of alerts, inquires, or issues.
b. Response capability.
c. Response time.
d. Response effectiveness.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The agency can't easily prepare and organize responsive resources for events not known or not likely to occur. Election administrators are expectedly quite occupied with regular responsibilities at this time.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. If the activity and resource can be made available (with modification as indicated) if it appears to have been helpful and useful this year.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop and implement an Election Day cybersecurity technical support program by April 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will develop an Election Day cybersecurity technical support program report and after action review with key partners by October 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Cybersecurity Public Education and Awareness

Deliverable: Election Cybersecurity Public Education and Awareness

General Information

1. **What is the deliverable?**
    a. Election security public education programming and coordination.

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better informed public and news media. Capability for timely and accurate messaging.

6. **What metric or measurement will be used to define success?**
    a. Creation of content and communications plan. Assessment of public and news media knowledge and confidence in election security.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Elections sector, the general public, and the news media.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Communications, Public Awareness, Policy, Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Secretary of State.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Ongoing communications initiative to inform and reassure the public about government's awareness and management of the cyber threat environment.	Secretary of State	75%	October 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2 - 3	1	Comm. Prof.	Agency	Fed. HAVA	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Maintaining public confidence in elections. Providing accurate information or responses to "fake or politicized news." General public understanding of the cyber threat environment.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This can improve/protect public perception of ongoing and existing cyber initiatives in place that are related to elections.

19. What is the risk or cost of not completing this deliverable?

a. Uncertain public confidence in state election administration.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success would be measured by the preparedness of content distribution and the quality of the information being released.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?
   a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?
   a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?
   a. Allocation of agency fiscal and human resources.

26. Who has the committee/working group contacted regarding implementing this deliverable?
   a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?
   a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?
   a. Combination of Technical, Communications and Executive leadership.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?
   a. Yes.

30. What are other public relations and/or marketing considerations to be noted?
   a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop a communications plan specific to election security by April 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will measure the success of communications plan efforts specific to election security by October 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Cybersecurity Incident Response and Communications

Deliverable: Election Cybersecurity Incident Response and Communications

General Information

1. **What is the deliverable?**
   a. Organize an election cybersecurity incident communications and response network.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Capability to rapidly communicate a cyber incident or threat information across the election sector and allied cybersecurity interests, and coordinate response activities.

6. **What metric or measurement will be used to define success?**
   a. Identify participants. Obtain participant acknowledgements and protocol agreements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. The election sector and general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Service, Energy, Communications, Public Awareness, Emergency Services, Cyber Sharing, Pre to Post Incident, and Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Secretary of State and Election Division, IDHS, DHS, State IOT and IN-ISAC, county and municipal units.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Establish and operate an Election Day cyber threat and incident response information and communications resource.	Secretary of State	100%	October 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1-2	0.25	General IT and Comm.	Agency	N/A	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Provide support to counties on identified issues and provide assurances to constituents that elections are well managed and secure.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable is intended to reduce the adverse impact to any identified/known issues. There are no direct costs associated with risk reduction.

19. What is the risk or cost of not completing this deliverable?

a. Unaddressed public concern that elections are not secure.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be defined in multiple parts: 1) the preparedness of the team in the event of an incident. 2) The quality of the resource as it relates to proper communications/support. 3) How effective the resource proves to be post-implementation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Allocation of agency fiscal and human resources.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop and distribute an Election Day cybersecurity incident communications and response to all Indiana election county officials by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

General Information

1. **What is the deliverable?**
   a. Collection of relevant election security reports and guides, indexed, summarized and periodically updated. Place on a website for Indiana election sector use.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

   ☒ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Uniform library of relevant information and guides, indexed and summarized, for reference and use across the election sector.

6. **What metric or measurement will be used to define success?**
   a. Posting the materials, index and summaries on web page and notifying the election sector.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Collection of materials with summaries	Secretary of State	75%	October 2018	

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No.

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. None.

Benefits and Risks

17. **What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)**
    a. Uniform library of relevant information and guides, indexed and summarized, for State, county and local election officials and administrators to reference and use.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. Effective situational awareness and familiarization with best practices and approaches. Increase uniformity of knowledge and practice across the sector.

19. **What is the risk or cost of not completing this deliverable?**
    a. Risk is operating on outdated information as well as inefficiency due to duplication of time and resources spent surveying reports and literature.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Availability of summarized collection of relevant reports and articles at an easily accessible location. Reduce the number of relevant reports and guides from approximately 50 to the "top ten" reports and guides.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Unknown.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Unknown.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Few if any. Election officials, administrators and staff are periodically preoccupied with ongoing Elections (i.e. May Primary and November General Elections in 2018).

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. Allocation of agency funds and human resources.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State and county election officials and administrators, allied IT staff and vendors.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop an election cybersecurity library by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Center for Internet Security (CIS) Handbook for Elections Infrastructure Security
- Department of Homeland Security (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC) ISAC Pilot for Election Infrastructure
- Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) Common Cyber Security Language
- Election Assistance Commission (EAC) Glossary of Common Cybersecurity Terms
- Election Assistance Commission (EAC) U.S. Election Systems as Critical Infrastructure Addendum I: Glossary of Key Terms and Acronyms
- Harvard Kennedy School Belfer Center Campaign Cybersecurity Playbook
- Harvard Kennedy School Belfer Center Election Cyber Incident Communications Coordination Guide
- Harvard Kennedy School Belfer Center The State and Local Election Cybersecurity Playbook
- National Association of Elections Officials Election Center Elections Security Checklist
- Voting System Technical Oversight Program at Ball State University (VSTOP) Indiana Best Practices Manual for the Operation of Election Equipment
- Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot
- Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot Report

Center for Internet Security (CIS)
Handbook for Elections Infrastructure Security

February 2018

Version 1.0 February 2018

Center for Internet Security®

A Handbook for

Elections Infrastructure Security

Center for Internet Security®

About CIS

CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

Center for Internet Security®

31 Tech Valley Drive
East Greenbush, New York 12061

T: 518.266.3460
F: 518.266.2085

www.cisecurity.org
Follow us on Twitter @CISecurity

A Handbook for

Elections Infrastructure Security

https://www.cisecurity.org/elections-resources/

Acknowledgments

CIS would like to recognize the following individuals and organizations for their support in creating this handbook. Their time and expertise were invaluable in completing this important work.

CIS authors

Brian Calkin
Kelvin Coleman
Brian de Vallance
Thomas Duffy
Curtis Dukes
Mike Garcia
John Gilligan
Paul Harrington
Caroline Hymel
Philippe Langlois
Adam Montville
Tony Sager
Ben Spear
Roisin Suver

Community contributions to and review of the handbook

Joseph Lorenzo Hall
Center for Democracy and Technology

Noah Praetz
Cook County, Illinois

Adam Ambrogi
Democracy Fund

Mike Goetz
Election Systems and Software

Tim Mattice
The Elections Center

Peter Lichtenheld
Hart InterCivic

Yejin Cooke
National Association of State CIOs

Susan Frederick and Danielle Dean
National Conference of State Legislators

Tim Blute and David Forscey
National Governors Association

Joshua Franklin and Gema Howell
National Institute of Standards and Technology

Emefa Agawu and Ian Wallace
New America Foundation

Tony Adams
Secure Works

Daniel Kambic and Greg Shannon
Software Engineering Institute

Trevor Timmons
State of Colorado

Robert Giles and Kevin Kearns
State of New Jersey

Tom Connolly
State of New York

U.S. Department of Homeland Security

Ryan Macias and Matt Masterson
U.S. Election Assistance Commission

David Mussington
University of Maryland

J. Alex Halderman
University of Michigan

Marian Schneider
Verified Voting

Contributions of current best practices

In addition, we'd like to thank the following individuals and organizations for providing examples of best practices in use today.

Beth Dlug
Allen County, Indiana

Emmit Lamb
Clark County, Nevada

Chris Chambliss
Clay County, Florida

Scott Konopasek
Contra Costa County, California

Kyle Rulli
Douglas County, Colorado

Stan Bethea
Duval County, Florida

Mark Earley
Leon County, Florida

Joe Miller
Linn County, Iowa

Bill Burgess
Marion County, Oregon

Faith Lyon
Portage County, Ohio

Ricky Hatch
Weber County, Utah

Part 1: **Introduction**

How cybersecurity and elections intersect and why it matters.

To enable the elections that define democracy, we must protect the security and reliability of elections infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand what to focus on, know how to prioritize and parse the enormous amount of guidance available on protecting information technology (IT) systems, and engage in additional collaboration to address common threats to this critical aspect of democracy.

The Center for Internet Security (CIS) and its partners publish this handbook as part of a comprehensive, nationwide approach to protect the democratic institution of voting. Election officials have been working diligently to secure their systems but, like so many other sectors, the threat to national security rises above any individual organization; we can accomplish more together, and we all share the same goal of free and fair elections. To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a national response to threats against elections infrastructure. This handbook addresses cybersecurity-related aspects of elections systems.

Background and purpose

Elections are the bedrock of democracy. Even before the establishment of the United States, adversaries sought to corrupt, interrupt, or otherwise disrupt democracy by subverting elections. From adversarial nation states, to terror groups, to Boss Tweed vote strikers, to those simply wishing to wreak havoc, attacks on the voting process are as old as voting itself. There is no way around it: protecting democracy calls for protecting elections.

The desire of some to disrupt elections has not changed; Joseph Harris's 1934 seminal book on elections, *Election Administration in the United States,* enumerates a series of election fraud incidents throughout American history. What is different in recent years is some of the tactics of such efforts to undermine democracy. Attacks leveraging weaknesses in digital infrastructure now augment traditional approaches and have become an increasingly common approach.

Judging by activity in industries and sectors outside elections, this should come as no surprise. Organizations across all sectors and government entities alike face daily attacks from actors with widely varying levels of sophistication. The most capable, best protected organizations have specific plans for addressing evolving threats. The plans are never static; these entities continually adapt—as do their adversaries—requiring an ongoing investment in security.

Moreover, in many industries and sectors, the good guys have realized that a go-it-alone strategy isn't enough. They've developed approaches that allow them to share information, establish best practices, and develop coordinated response plans to mitigate effects of coordinated attacks. This collaboration raises the level of security for the individual organizations, their respective industries or sectors, and the country.

Even in the financial services industry—in which annual investments by individual organizations in improved security for their digital systems can range in the many hundreds of millions of dollars—organizations pool some resources to support the Financial Services Information Sharing and Analysis Center. This collaborative approach to monitoring the evolving threat environment helps support even the most substantial individual efforts. These same approaches have been repeated in many industries, including communications, the defense industrial base, aviation, oil and gas, real estate, electricity, and others. Protecting elections infrastructure is certainly no less important to our country's national security and overall well-being than protecting the infrastructures in these other vital sectors.

In the state and local sector, the Multi-State Information Sharing & Analysis Center (MS-ISAC) works with state and local entities to monitor threats to their systems, detect common attacks across states, and support mitigation of risks presented by vulnerabilities and changing attacker behavior. This results in a more rapid deployment of solutions when new threats emerge; if there's one thing we know about these actors, once they succeed in an attack, they'll duplicate it everywhere they can.

The parent organization of the MS-ISAC and sponsor of this handbook, CIS, has used collaboration among a large number of security experts as a means to identify best security practices. These collaborative processes have resulted in several products available to state and local governments and other entities, including election officials and their technical staff. These include the CIS Controls and CIS Benchmarks, which heavily inform the recommendations in this handbook.

An underlying reality to all current work in cybersecurity is that a skills gap exists for cybersecurity globally, across all industries—elections included. Closing this skills gap is critical to elections and securing the process. Implementing best practices is only possible with the right people who have the necessary skill-set. Therefore, we hope what follows in this handbook will serve individuals with differing skills and resources in implementing practical guidance for election administration.

The elections environment

Elections in the United States are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the federal government provides some laws and regulations, states have substantial discretion on the process of conducting elections. The federal government does not administer elections and has a limited role in dictating how the process is to be conducted.

States act as the primary authority for the laws and regulations that govern the process of conducting an election in that state. Under federal law, states must designate a chief state election official. This official typically sets rules and regulations for the implementation of election technologies and their use. Although states are heavily involved in setting the rules and policies for administering elections, and in choosing election technology, in most states local jurisdictions administer and conduct the processes of an election.

Many local jurisdictions have the ability to procure their own election technology from a set of certified or approved manufacturers and vendors designated by their respective state. Additionally, the local jurisdictions are typically responsible for inventorying, securing, and training staff on those technologies. Depending on the size and resources of the jurisdiction, the number and technical skills of the staff can vary greatly, ranging from an elections team with its own dedicated IT and security personnel to a single person with little to no IT background. Many elections offices rely on IT resources shared with other administrative functions (e.g., other county agencies) or rely exclusively on technology providers (e.g., elections and IT systems vendors) for implementing and securing their election infrastructure. This can result in dependencies that are outside of the local officials' control.

Audience

By using this handbook, we hope election officials and those that manufacture, own, operate, or are otherwise involved with elections systems and their IT components are better able to understand and prioritize risks, understand best practices that can identify threats, detect attacks, allow for recovery from cybersecurity incidents, and, ultimately, continue to provide and support systems for the execution of free and fair elections.

In addition to this handbook providing a path to continually evolving security, perhaps the most important aspect of this effort is to help instill a continued sense of faith in elections by voters themselves. We hope election officials are able to use this handbook to highlight the past and ongoing work they've done to secure the elections process and that, through openness, transparency, inclusion of relevant stakeholders, and consideration of the entirety of the elections process, voters recognize that democracy is working and their votes will count.

More specifically, we hope this handbook is of use to each of the following:

- **Election officials and senior executives.** These individuals are accountable for executing elections. In addition to state and local election officials, they may include those indirectly involved in the election process, such as the offices of legislators and governors.
- **Owners and operators of elections systems.** These individuals have more responsibility for the systems themselves, though there may be some overlap with election officials. It's critical that they understand the risk context and the technical guidance in this handbook.
- **Vendors of hardware and software.** Whether providing systems and services dedicated to elections or general purpose but used in elections, vendors are, and must remain, partners in this process. Moreover, vendors often provide the primary technology expertise and labor to local election officials. Vendors have a vested interest in their products and services, and election officials driving vendors toward best practices can help all boats to rise with the tide, including improvements in the development, testing, and continual evolution of vendors' products.
- **Others who can help secure elections.** This includes the U.S. Election Assistance Commission (EAC), the U.S. Department of Homeland Security (DHS), state chief information officers and chief information security officers, state homeland security advisors, fusion centers, election integrity groups, academics, and other non-profits and private companies willing to lead or support various efforts. This is, in many ways, a baselining effort that we hope supports other efforts dedicated to improving the security of elections, both new and ongoing.
- **Voters, the media, and other interested stakeholders.** In the end, no stakeholder matters more than voters. Not only is it the duty of all to ensure elections represent the will of voters, but it is the duty of all to ensure that voters have confidence in the process before heading to the polls and after results come in.

Goals and outcomes

This handbook is about establishing a consistent, widely agreed-upon set of best practices for the security of systems infrastructure that supports elections. It provides both a general explanation of the threats that exist for the various components of the elections process and examples of known mitigations for these threats.

By developing and publishing this handbook, CIS aims to establish a baseline of protection for all aspects of the elections infrastructure ecosystem that leverage digital tools and applications.
The primary goal of this handbook is to impact and improve the security of elections infrastructure as soon as possible, and ideally in advance of the 2018 elections, and establish a set of best practices that, with continual updates, supports elections infrastructure security into the future. We expect many elections systems will already incorporate the majority of these mitigations, allowing those jurisdictions to demonstrate a strong baseline. In that case, the handbook can assist in prioritizing for continual improvement and evolution.

Handbook structure

This handbook is divided into three parts that together provide a baseline view of how to manage cybersecurity risk in elections:

- **Part 1: Introduction.** This introductory section describes this handbook and providessome general information on risk assessments in elections systems.
- **Part 2: Elections Systems and Risk**. The second part **introduces a high-level generic elections architecture,** some components of which may exist at the state level, some at the local level, some both, and some not applicable in certain jurisdictions. It also **classifies these common components of elections systems according to the manner in which they are connected to networks or other systems.** For each major component of the generic elections infrastructure, there is an overview and description of how it fits in the elections landscape and a brief description of the risks and

threats associated with the component. Finally, it summarizes the classification-based ways that different implementations of the components are connected to other digital infrastructure.

- **Part 3: Mitigating System Risk.** The third part is a **technical best practice guide that provides controls and recommendations for systems.** It includes two major sections: 1) a set of critical risk-mitigating activities that can benefit any organization and 2) a set of technical best practices for users, devices, software, and processes that are listed first for components that are network connected and then for those that are indirectly connected. We also provide technical best practices that address transmission of information among digital components of the elections infrastructure. As described below, the nature of the connectivity to other elements of the elections digital infrastructure is the major security vulnerability area and thus we have chosen this connectivity as the basis for organizing technical controls. Technical staff, whether government or contracted resources, should be able to implement these controls to provide an appropriate mitigation of risk.

What this handbook is not

A shortcoming of many efforts in domains as large as IT security and elections is a failure to properly scope efforts. In addition to describing what this handbook is, we want to be explicit about what this handbook is not.

Aspects of elections, voting, and protecting democratic institutions that are not part of the scope of this handbook are not an indication of importance, but rather an acknowledgment that no single effort can successfully address everything. This handbook limits its scope to only digital aspects of elections themselves, though in some cases it references paper-based processes in order to further the discussion. The one exception to this is the recognition of how the means of transmission can inject cybersecurity risks, such as digitally transmitting to-be-paper pollbooks to a printer. In these cases, we identify the transmission risks in Part 2 and the mitigations to transmission risks in Part 3.

Beyond this, there are several aspects of election security we do not address. This handbook is not:

- **A one-size-fits-all.** This handbook **does not recommend any single approach to managing election systems or developing and deploying elections systems technology.** Election jurisdictions tailor their voting processes and systems to the needs of their voters and jurisdictional laws and requirements. That said, there are many commonalities. Rather than focus on differences of approach, this handbook focuses on the best practices associated with common approaches, recognizing the variety of approaches and architectures wherever possible.
- **An all-encompassing scope.** As this handbook is about improving the security of elections infrastructure as it exists today, **we have intentionally left several aspects of the broader voting process, however important, out of scope:**
  - Eligibility for an individual to register to vote;
  - Voter identity verification, unless specifically about the accuracy and availability of voter registration rolls;
  - Security of campaigns or campaign information systems; and
  - The accuracy of information about candidates or issues, including those conveyed using social media.

Assessing risk in elections systems

A common way of describing an organization's cybersecurity posture is in terms of risks that have been mitigated and risks that have been accepted. Those outside the information security community will often think of security in terms of stopping all possible threats. Both within the community and in the legal domain, practitioners understand that perfect cybersecurity is not possible. Rather, organizations seek to achieve "reasonable" security that involves accepting some level of risk given the threats and potential consequences, while maintaining an ability to recover should any of those consequences be felt.

Elections systems risk overview

The IT systems infrastructure that supports our elections processes has myriad risks, and these risks vary from one organization to the next. There are a number of commonly used risk assessment approaches that can be used by election officials and their technical staff to help assess risk, such as International Organization for Standardization (ISO/IEC) 27005 and National Institute of Standards and Technology (NIST) Special Publication 800-30. Among the most popular tools for understanding and managing cybersecurity risk is the NIST Cybersecurity Framework, which organizes cybersecurity activities in five functions: identify, protect, detect, respond, and recover.

Unfortunately, many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems.

In its simplest form, a risk assessment is used to identify and assess the impact of vulnerabilities—weaknesses that an attacker can exploit—while being mindful of the compensating controls that exist in a system. These risks can be mitigated with appropriate physical, process, and technical safeguards. In this way, risk and potential impacts can be reduced to a level deemed acceptable by the accountable election officials, often called a balanced risk posture. The potential impact or consequence of a successful exploit is an important part of a risk assessment as elections officials want to focus first on exploits that have the greatest potential consequence. While some risks vary from one election jurisdiction to another, many are common across the wide variety of elections systems configurations. As part of producing this handbook, experts have collaborated to assess the common risks to elections systems. This common baseline risk assessment has influenced the prioritization of security best practices in the handbook.

Baseline elections risk assessment

The baseline assessment of risk for elections is summarized for the purpose of helping election officials and their technical staffs understand the major areas of risk that can serve as their primary focus. Each organization should augment the baseline elections risk assessment to address the risks that might be unique to their elections processes, systems, and threats.

Examples of threats and consequences

Scenario 1:
A nation-state uses the internet to access and disrupt one or more state voter registration databases such that legitimately registered voters are denied the ability to vote on election day, or are required to file a provisional ballot.

Consequence:
Although no votes are manipulated, this attack would likely be a major national news story that results in reduced confidence by the public in the integrity of the voting process and the election results. Additionally, this slows the voting process, creating the risk of long lines and making in-person voting less efficient.

Scenario 2:
An adversary gains access through the internet to one or more election night vote displays and changes the displayed results such that the real winner of the election is now the reported loser in the election.

Consequence:
Again, while no votes have been changed, and the erroneous posting of election results by an authoritative source will subsequently be republished correctly, there is likely to be a significant loss of voter confidence.

A top-level assessment of vulnerabilities and potential consequences to the elections systems infrastructure identifies network connectivity—devices or systems that work with other devices or systems to achieve their objectives—as the major potential vulnerability. The reason is simple: given an adversary with sufficient time and resources, systems that can be accessed via a network cannot be fully protected against compromise. There are ways to improve the security of network connected systems with additional controls, but the inherent complexity of network connectivity results in significant residual vulnerabilities.

Therefore, risks for system components that are connected to a network should be treated differently than for components that are never connected to a network. In this handbook, the definition of "network" includes connections to the internet as well as connections to both local wired and wireless networks.

While systems that are continuously connected to a network have a somewhat higher risk than systems that are only intermittently connected to a network, experts have demonstrated that any network connectivity, even if only for a limited period of time, results in a significantly larger vulnerability profile. An access path to these components may be available through the internet if any connected component can access the internet, and thus an attack can be orchestrated from anywhere in the world. The box to the right illustrates examples of these threats.

On the other hand, systems that have a digital component but are not network connected have a reduced vulnerability profile. Specifically, there are fewer ways to attack such systems and devices, but it does not mean the consequences of a successful attack are any lower—indeed, an attack can still be executed without geographic boundaries. The methods used to upload and download information (e.g., USB sticks, memory cards) still have vulnerabilities, but there are fewer vectors of attack to mitigate.

Three classes of elections systems

In this handbook, we have organized best practices into two classes based on the different threat characteristics associated with levels of connectedness. A third class, that of processes that are executed without a digital component, such as hand-counted paper ballots—the casting and counting of ballots via purely paper and manual means—is out of scope for the handbook.

While there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analyzing the manner in which they connect to networks and other devices. Throughout this handbook, we classify components of elections systems based on three types of connections that most clearly define the risk landscape:

1. **Network connected systems and components.** Network connected components are interconnected with other devices to achieve their objectives. The level of interconnection, while providing various benefits, also introduces additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means organizations must make extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. As an example, an Election Management System (EMS) connected to a private county network would still be classified as a network connected system.

2. **Indirectly connected systems.** Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, have to exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives or other flash media. While the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive.

3. **Non-digital elections components.** These are aspects of the elections process that have no digital component and are **out of scope for this handbook.** An example would be the mailing, completing, and returning of a paper mail-in ballot. While aspects of the overall process—such as an online request for the ballot—may leverage digital infrastructure, the aspect of this process that is purely paper-based is out of scope.

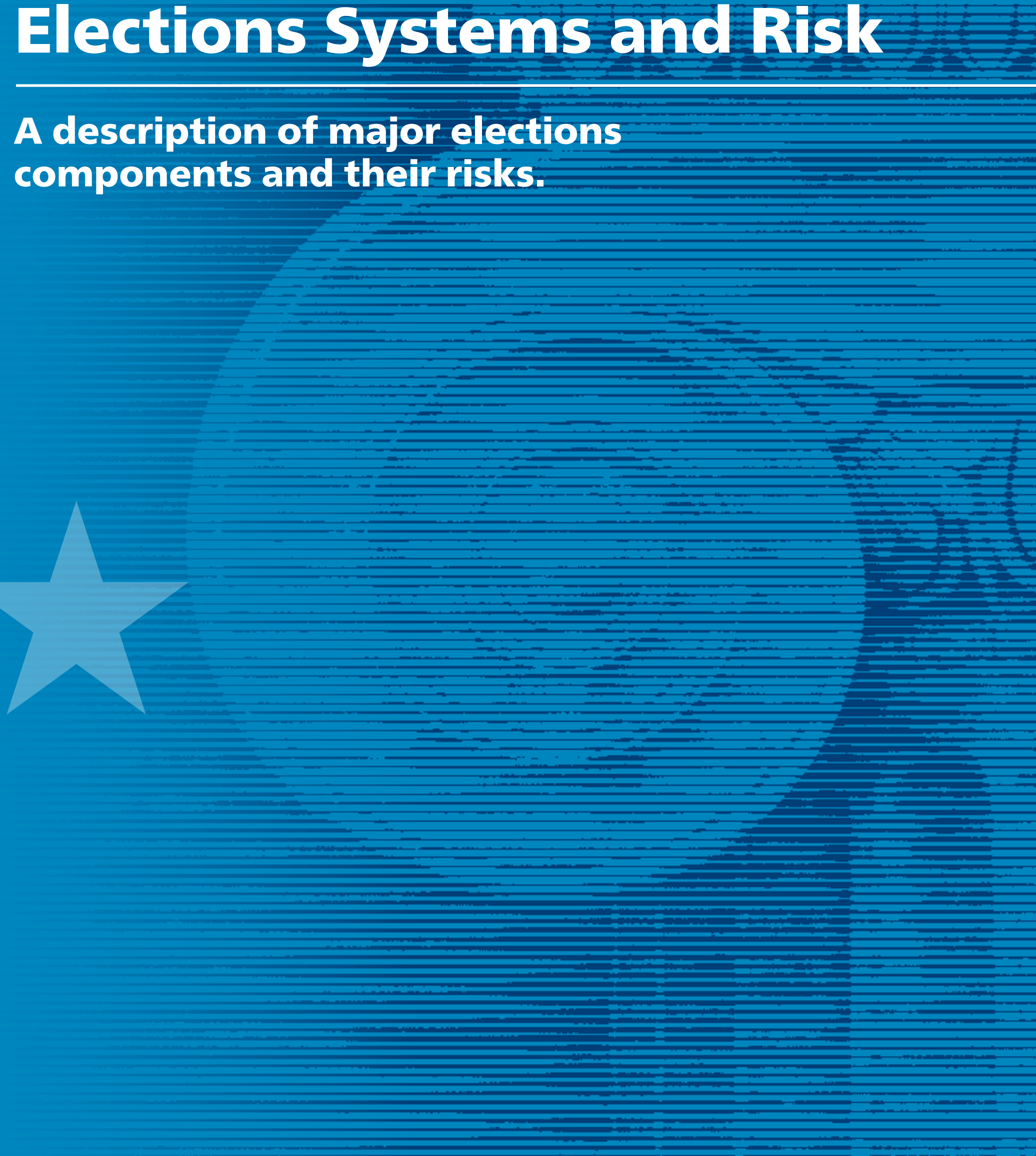
In Part 2 of the handbook, each major component of an election system is briefly described and then placed into one of these classes, providing a method to simplify the risk landscape and assist officials and their technical staff in determining the most effective and efficient approaches to managing risk. In some cases, major components are divided into the primary approaches to executing a process, such as the different approaches to conducting vote capture, each of which is classified individually. This classification analysis becomes the foundational basis for an elections organization selecting the appropriate technical best practices for that component described in Part 3 of the handbook.

Transmission between components creates vulnerabilities

While securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack—attack vectors in cybersecurity parlance—lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected. For instance, while paper pollbooks wouldn't typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks that must be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e., vote capture) devices. In Part 3, we also address transmission risks of this nature and the best practices that can mitigate them.

Part 2: **Elections Systems and Risk**

A description of major elections components and their risks.



This part of the handbook provides a generalized elections systems architecture showing each major component of the systems and:

1. A discussion of the risks and threats for each major component,
2. For some components, a description of the different types of deployment in use, and
3. A classification of the component based on how it connects to other devices, and thereby a mapping to controls and recommendations in Part 3 of this handbook.

A generalized elections systems architecture

There are many flavors of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. That said, many experts have studied the elections process at length, and there are several fundamental components common to nearly all elections systems.

In some jurisdictions, the owner of various aspects of the architecture may differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices. Those accountable for elections infrastructure should understand these basic processes and identify the parts where they have purview. A description of major system components that comprise the elections infrastructure are shown in [FIGURE 1].

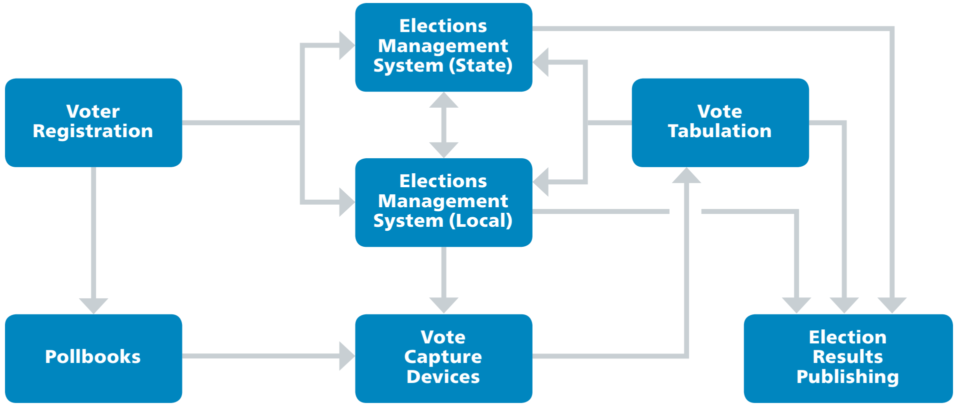

Elections Management System (State)
Voter Registration
Vote Tabulation
Elections Management System (Local)
Pollbooks
Vote Capture Devices
Election Results Publishing

FIGURE 1: *A generalized elections systems architecture*

While each of these systems has IT components that require security best practices, this handbook addresses a subset that are, in our view, the highest risk targets of attack by adversaries and thus require the bulk of the attention. For digital components not covered in the handbook, the analysis methods used here can be applied to determine the appropriate set of technical best practices for that component.

Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components may exist at the state level, at the local level, or both, and some will not be applicable in certain jurisdictions. Nonetheless, all will exist in most jurisdictions and must be addressed in order to provide a comprehensive best practices guide. This is especially true for local jurisdictions, given the extent to which elections are administered locally. Even where there is a substantial amount of legacy infrastructure—old systems that are difficult or impossible to update—much can be done to mitigate risks. These systems are described below and appropriate best practices and controls are provided in Part 3.

Voter registration

Every state has a unique approach to voter registration—including some states with automatic voter registration—but there are several commonalities shared by all of them. Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks—paper and electronic—as well as provide information back to the voter as they verify their registration and look up polling locations and sample ballots.

The inputs to voter registration systems are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state. The outputs include facilitating voter lookups—such as a voter verifying they are registered, seeking a sample ballot, or finding their polling place—and transfer of voter information to pollbooks.

In all of these cases, there is a master voter database at the state level. The 2014 EAC Statutory Overview describes this database as populated in one of three broad ways:

1. A top-down system in which the data are hosted on a single, central platform of hardware and maintained by the state with data and information supplied by local jurisdictions,
2. A bottom-up system in which the data are hosted on local hardware and periodically compiled to form a statewide voter registration list, or
3. A hybrid approach, which is a combination of a top-down and bottom-up system.

For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on commercial-off-the-shelf (COTS) hardware and software. Because they use these common computing platforms, voter registration systems may be part of a shared computing system, though in many cases they are dedicated systems with dedicated software.

While jurisdictions vary in how they allow voters to apply or update their registration, in many states, the most common way voters access a registration system is through the state's department of motor vehicles (DMV).

Additionally, voters' connection to the voter registration system may run through direct means such as a county or state registration portal, or through indirect means like mailing in a registration on paper. To address this risk, many voter registration systems with which the voter would interact are separated from the "official," or production, voter registration system. Periodically, a report of changes is generated and undergoes a quality assurance review that must be certified before being entered into the production system. This can substantially reduce, for instance, an online portal as a vector of attack, though the production system may still be network connected in other ways.

In general, voter registration systems exhibit the risk characteristics of a general-purpose computing system and, more specifically, any network connected database application. To properly mitigate risks, each voter registration system within a state, and links to the voter registration system, needs a comprehensive assessment of its technical characteristics and the application of appropriate security controls.

[FIGURE 2] shows the major functions or subsystems of a voter registration system.

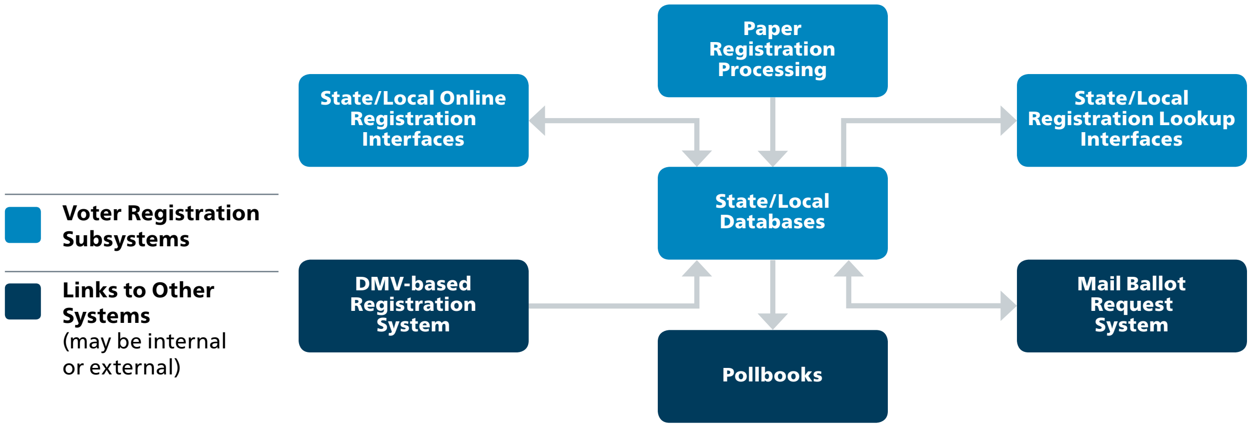

Voter Registration Subsystems
Links to Other Systems (may be internal or external)
Paper Registration Processing
State/Local Online Registration Interfaces
State/Local Registration Lookup Interfaces
State/Local Databases
DMV-based Registration System
Mail Ballot Request System
Pollbooks

FIGURE 2: *Components of a typical voter registration system*

Types of voter registration

Voter registration generally occurs in one of two ways, each of which is recorded in a statewide registration system.

1) Online registration: a website or other web application allows prospective voters to register electronically and have election officials review their registration for validity, which, if valid, is entered into the voter registration database. Same-day registration, because of the need for live updating and cross checking, usually falls into this category.

2) Paper-based registration: prospective voters submit a paper voter registration form that is reviewed by election officials and, if valid, entered into the voter registration database. Registration of this type is out of scope in this handbook.

The type of voter registration employed at DMVs will vary by state—and perhaps locality—but should typically be viewed as a form of online registration.

Risks and threats

As noted in the previous section, the ability to access voter registration systems through the internet results in a significant increase in vulnerability and resulting risk. There are well known best practices to mitigate these risks such as those described in the box to the right, but the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components.

While the attacks on voter registration systems may have a specific purpose not found outside the elections domain, the vectors for those attacks, and thus the primary risks and threats associated with voter registration systems, are similar to those of other systems running on COTS IT hardware and software, and include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These items must be managed to ensure proper management of voter registration systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats. Based on their type of connectedness to digital systems, these controls are listed in Part 3.

In practice: protecting the voter registration database

Cybersecurity practitioners constantly face a difficult balance between convenience for users and strong security. With voter registration databases, some approaches allow elections officials to have it both ways.

Practice #1:
Officials in Washington State leverage what's called a "sneakernet" to move information from an internet-facing copy of the voter registration database and a master version of the database that is not connected to the internet. Officials have to physically move data from one machine to another—usually by moving their sneakers to walk it across the room. This doesn't eliminate all risks, but can help protect sensitive information from attack through internet-based vectors, while still allowing individuals to access their information over the internet.

Officials can only access the database from a special application. This application makes periodic copies of the database in a tightly controlled environment and these copies are used to populate all other interfaces. Similarly, changes to the master database are limited to this application. So updates from, say, the DMV don't directly access the database. They're carefully checked for corruption and moved to the master database through this controlled process.

Practice #2:
Some jurisdictions don't air gap their master voter database but use other methods to balance strong security and real-time election official access to the database. In Colorado, the master database is accessible via networks due to needs such as facilitating same-day registration. Experienced cybersecurity professionals leverage appropriate protections including strong vulnerability and risk management programs coupled with robust access controls, intrusion detection and prevention systems, web application firewalls, and security information and event management integration. Multiple layers of defenses—both computerized and human—are used to sustain operations while minimizing risk.

How these components connect

Each type of voter registration, along with the master voter registration database, should have risks evaluated individually based on its type of connectivity and employ controls and best practices found in Part 3 that correspond to the type of connectivity and are appropriate to address risks. That said, aspects of the voter registration systems, and the types that may be implemented, have general characteristics that can be classified by connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

1) Online registration.

In addition, the master registration database or system itself should be considered network connected.

Indirectly Connected

N/A

Not connected, out of scope

2) Paper-based registration.

Additional transmission-based risks

Transmission of a registration via email or fax leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3.

Pollbooks

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this section focuses primarily on electronic pollbooks (e-pollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These e-pollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These e-pollbooks are typically dedicated software built on COTS hardware and riding on COTS operating systems.

The primary input to e-pollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, e-pollbooks may require additional inputs and outputs to allow for election day changes.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer—whether at the state or local level, or via commercial printing services—protects the integrity of the information in printed pollbooks.

Risks and threats

Attacks on e-pollbooks would generally serve to disrupt the election day process by one of these three situations: 1) attacking the integrity of the data on the pollbook by altering the information displayed from voter rolls, 2) disrupting the availability of the e-pollbooks themselves, or 3) in some cases, causing issues with the vote capture device by altering an activation token. Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that prevents them from casting a ballot or forces them to use the provisional ballot process, but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook.

An e-pollbook may or may not be connected to a network. If they are network connected, they must be treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an e-pollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for e-pollbooks,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact.

These primary risks must be managed to ensure proper management of pollbooks. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Managing risks associated with e-pollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

Pollbook connects via a wired or wireless network.

Indirectly Connected

Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).

Not connected, out of scope

Paper-based pollbooks.

Additional transmission-based risks

Transmission of data for paper-based pollbooks for formatting or printing. If this transmission incorporates a digital component, it should incorporate the relevant transmission-based mitigations in Part 3.

State and local Election Management Systems

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A state EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of this handbook, vote tabulation is broken out into its own section.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties between the state and the local jurisdictions and the manner in which each state or local jurisdiction handles particular aspects of the election process.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware that operate in a networked environment. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

Significant consequences may result from successful attacks on an EMS. These potential consequences include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a state or local EMS is network connected and whether communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP). Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

Unless known definitively to have no network capabilities, treat an EMS as network connected.

Indirectly Connected

If known definitively to have no network capabilities, treat an EMS as indirectly connected.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Vote capture

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place may give voters the choice of electronic machines or paper ballots. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

To this end, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other federal partners, state and local governments, vendors, and others in the elections community, maintain standards and a certification program for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a generalized set of recommendations that can help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security—and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But, as documented throughout this handbook, they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

The primary inputs to vote capture devices are the ballot definition file—which describes to the device how to display the ballot—as well as an activation key (for some electronic machines) and the ballot itself for scanning of a paper ballot. The primary output is, of course, the cast vote record.

In cybersecurity, we often talk about non-repudiation: the inability to deny having taken an action. Our democracy is founded in the opposite principle: your ballot is secret; no one should be able to prove who or what you voted for—or against—in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. We intentionally create voter anonymity through a breakpoint between the fact that an individual voted and what votes they actually cast. We never want to enable the ability to look at a marked ballot and track it back to a specific voter.

Instead, we must carefully protect the integrity and secrecy of the vote cast through the capture process and into the process of tabulation. To do this, best practices call for applying a series of controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

Principles and more through the VVSG

The EAC is currently in the process of developing the Voluntary Voting System Guidelines (VVSG) version 2.0. The draft recommended by NIST and the EAC's Technical Guidelines Development Committee incorporates many of the best practices described within this handbook, such as auditability, access controls, data protection, system integrity, and detection and monitoring. The recommended draft is written as a high-level set of principles and guidelines, allowing specific requirements to change without requiring the full EAC approval process. This provides nimbleness and flexibility in voting systems and their underlying cybersecurity as requirements can be developed and mitigations implemented as threats are identified. More information about the VVSG 2.0 development and proposed draft can be found on the EAC's website.

Types of vote capture processes

Vote capture generally occurs in one of six ways:

1) **Voter marked and hand counted paper balloting.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.

2) **Voter marked paper balloting with scanning.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots.

3) **Electronic marking with paper ballot output.** Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a *ballot marking device.*

4) **Electronic voting with paper record.** The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a *direct record electronic (DRE) device with voter verifiable paper audit trail.*

5) **Electronic voting with no paper record.** The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as a *DRE device.*

6) **Electronic receipt and delivery of ballots conducted remotely.** The majority of ballots received by voters using this method are voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Though most UOCAVA votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. When this approach is used, the balloting itself is out of scope as it is via paper means. However, this type of voting can carry transmission-based risks.

Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject—in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, a state or local entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The type of vote capture device we call *electronic receipt and delivery of ballots conducted remote*ly can take on a large number of flavors. In terms of cybersecurity-related risks, for activities like emailing ballots, election officials must consider especially risks involved in the transmission of the ballot. Whether during distribution or return, if the transmission of the ballot is done via digital means, it is subject to the risks of that transmission mode. In Part 3, there is a set of control measures that provide mitigations for risks in transmission.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- If ever networked, risks associated with established (whether persistent or intermittent) network connectivity,
- Risks associated with the corruption of removable media or temporary physical connections to systems that are networked,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network.

Also, many central count scanners, used for *Voter marked paper balloting with scanning* in batches (usually vote by mail ballots) are similarly networked on a closed-LAN.

Some electronic vote capture machines also directly transmit data for election night reporting.

Indirectly Connected

2) *Voter marked paper balloting with scanning.* Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
3) *Electronic voting with paper ballot output.* In addition to the role of the scanners, the vote capture machines are typically not network connected, but must be programmed to display the ballot and print the ballot in the correct format.
4) *Electronic voting with paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
5) *Electronic voting with no paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.

NOTE: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Not connected, out of scope

1) *Voter marked and hand counted paper balloting.* Out of scope in this handbook as the vote capture process does not include a digital component.

Additional transmission-based risks

6) *Electronic voting conducted remotely.* These methods vary greatly and must be addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3. Aspects definitively executed without a digital component are *not connected, out of scope.*

Vote tabulation

In its broadest definition, vote tabulation is any aggregation or summation of votes. Vote tabulation is the aggregation of votes (e.g., cast vote records and vote summaries) for the purpose of generating totals and results report files. For the purposes of this handbook, this section on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Vote tabulation in this handbook is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g., results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across a network. Vote data is most often transferred across jurisdictions and to the state through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,

- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Lack of confidentiality and integrity protection for transmitted results,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These primary risks must be managed to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, vote tabulation equipment will be *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If vote tabulation equipment is not *network connected,* it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Election results reporting and publishing

After votes are tabulated, results must be communicated both internally and to the public. In any given state, this can take many forms, but, in most cases, the basic process goal remains: getting results as quickly and accurately as possible. This section focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing tabulated votes as described in the previous section. The systems used for reporting and publishing are likely networked, and, in many cases, have public facing websites.

The outputs are the unofficial election results, typically published on a website, often in multiple formats such as extensible markup language (XML), hypertext markup language (HTML), portable document format (PDF), and comma-separated values (CSV). There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results may be kept on a system that is not persistently connected to the internet.

How these components connect

Depending on the approach to submitting tabulated votes, the reporting component may be network connected. The publishing component is almost certainly network connected, but may be indirectly connected, depending on the implementation. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, election night reporting will be n*etwork connected,* whether through a wired or wireless connection.

The publishing component of election night reporting is almost certainly *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If the election night reporting process is not network connected, it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Part 3: **Mitigating System Risk**

Critical activities and best practices in elections infrastructure security.

Mitigating risk is, ultimately, about decisions and actions that establish trust in aspects of a system, leading to confidence in the outcome. Risk must be considered at every stage of a system – requirements, design, development, operation, and even for disposal or retirement (e.g., removal of sensitive information).

Like many systems, for election systems this involves establishing trust in users, devices, software, and processes. Many systems are "composed," or built up from a variety of commercial and purpose-built parts, devices, and software connected via processes and user actions. The results in security decisions about trust are made across many components and brought together at a system level. In other cases, key election system components or services functions are contracted out. This does not change the security responsibility for decision-makers, but forces them to think about how the desired security properties can be specified in contract language and service specifications, rather than implemented directly.

This part of the handbook contains:

1. A set of critical risk-mitigating activities from which all organizations can benefit,
2. Recommendations for best practices in contracting for IT services, and
3. A set of best practices in the form of recommendations and controls for network connected and indirectly connected devices, as well as for transmission of information.

Critical risk-mitigating activities

Auditing

Election officials conduct many audits of all aspects of the election process (e.g., vote by mail processing, training, equipment delivery) and election systems (e.g., voter registration transactions, audit log data). However, the focus of this section is on auditing vote capture and tabulation in an election.

Included in this is to validate that the aggregated results reflect the actual ballots cast. One auditing approach is to select a sample of the ballots and, applying a structured process, do a partial recount of the ballots. This controlled audit is intended to provide confidence that the voting results are accurate based on the results of that partial recount. Moreover, audits provide information to election officials that go beyond the requirements for audit and recounting results; audits are the "production time" opportunity for election officials to know that the systems they are using are working properly.

The approach to auditing can vary based on a number of factors, including requirements that may be established within elections jurisdictions. Some auditing requirements call for a manual recount of a set percentage of ballots, others—including risk limiting audits described below—leverage statistical methods to determine the extent of the recount. Auditing requirements typically also have a trigger for a larger recount or full recount based on the outcome of the initial audit. Given the potential expense of auditing, it is critical to properly design audit procedures to reduce costs while achieving the goals of the audit.

Objective auditing in Linn County

In Iowa, Linn County Election Services hired a cybersecurity firm to conduct an audit of various aspects of the county's elections infrastructure. The firm submitted recommendations, and the county decided which of those to prioritize for implementation. The goal in hiring a third-party vendor was to provide objective, professional advice and assistance. This helps ongoing security efforts and gives confidence to the public that Linn County is taking cybersecurity seriously in its elections.

Almost all states have provisions for a full recount of a contest should the result of that contest fall within the state required recount margin (for instance, many states require a recount for a statewide race if that race is within one half of one percent after certification).

The initial audit size and recount triggers are critically important to a good audit. As important is the method by which the audited ballots are selected. Establishing proper methods for random selection of ballots can have a tremendous impact on the audit's ability to confirm election results or show evidence of tampering.

For election officials, the first step to a good audit is recognizing that records must be kept in order to make an audit possible. This means allocating resources to support an audit, along with procedures for efficiently executing the audit and making it sufficiently transparent for interested parties. While audits are not inherently digitally-based efforts, establishing an audit process, with resources, ballot selection methods, audit size rules, and recount triggers, is a critical aspect of mitigating risk across all aspects of elections.

A best practice: risk limiting audits

A possible weakness in some traditional auditing methods is that often either more ballots or fewer ballots are recounted than necessary to validate the results. This can either produce an audit that doesn't fully validate the outcome of the election, or an audit that is more costly than necessary without increasing confidence in the results.

More recently, the concept of risk limiting audits has been introduced as an approach to auditing election results that is both effective and efficient. In addition to those characteristics necessary in a traditional audit—resources, good ballot selection methods, and prior-determined rules—in a risk limiting audit the size of the audit and recount triggers are based on a "stopping rule" determined by the likelihood that the actual election outcome differs from the reported outcome. Put another way, additional ballots are recounted in the audit until there is a pre-determined statistical level of confidence that the reported result is correct. As an example, a very large margin of victory will typically result in a relatively small audit size, as a very large error would have to occur to change the outcome. A very close election, on the other hand, would require a larger audit.

In practice: risk limiting audits in Colorado

Recently, the state of Colorado established a legal requirement that all elections be subjected to a risk limiting audit. The Colorado Secretary of State defines the "risk limits" for each election. The risk limits (i.e., the acceptable probability that the election results might not be correct based on the statistical analysis process implemented within the risk limiting audit) will guide the process of selecting the size and distribution of the sample to be subjected to the initial audit, and in turn successive audits if they are required to achieve the risk limit confidence. The trend of leveraging risk limiting audits continues to gain steam, and election organizations should consider Colorado as a use case from which they can learn. The References section of this handbook provides additional information on Colorado's approach.

In a risk limiting audit, the size of the audit is determined by the results of the audit itself. That is, the closer the audited results are to the actual outcome, the sooner the audit ends. This is termed the statistical confidence in an election's results. As soon as a previously-determined confidence threshold is met, the audit can stop. As in all audits, units—precincts, machines, batches of paper records—should be selected using random sampling methods. In a risk-limiting audit, the sample size will depend on the margin of victory and other factors; these other factors may include the number of ballots in each precinct and the overall number of ballots in the contests. In general, smaller margins of victory and fewer total votes cast require auditing a larger percentage of the ballots cast. These methods are well-documented and replicable through sources such as ElectionAudits.org.

Incident response planning

Despite the best efforts of election officials and their technical staff, there is some likelihood that there will be an incident at some point during an election cycle. This is the nature of cybersecurity; the true measure of success is often the resiliency of an organization in the face of these incidents.

Incidents can be minor, having no real potential for impacting the election results or public perception of the elections process, or they could be major incidents requiring prompt action to ensure the actual or perceived integrity of the election results. An incident could be a direct attack on some portion of the election system, or it could be a potential threat that might affect confidence in the system (e.g., a reported major flaw in a foundational COTS component of many election systems).

Experience shows that successful incident response depends almost entirely on planning and preparation—the work done before any incident occurs. Good technical and process controls will minimize the attack surface and also help to enable timely analysis of the incident. Identifying key decision-makers and their roles ahead of time allows for effective response.

Planning and preparing begins with creating a plan for diagnosing and recovering from incidents and exercising this plan. To properly develop and exercise these plans, efforts must include a wide variety of stakeholders—ideally all stakeholders that would be involved in response to and recovery from the incident itself. All stakeholders, including seemingly sovereign ones such as federal, state, and local officials, must collaborate in incident response and recovery; they must also collaborate in preparing for those incidents. As the threats change, so must plans. Officials must update documentation regularly and include specific plans for addressing modern cybersecurity risks, such as those presented throughout Part 2.

In practice: recovery ready in Cook County and California

In Illinois, since 2007, the Cook County Clerk's office has worked with an independent data analysis firm, Data Defenders, LLC, which has implemented its Applied Computer Forensics process, called Election System Auditing (ESA)™, as part of an overall election integrity management plan.

For each election, the forensics process takes three "snapshots" of the election equipment: one prior to pre-election logic and accuracy testing (Pre-LAT), one immediately after Pre-LAT, and a final one after the election has finished and the equipment is returned from the polling places and early voting sites.

These snapshots capture all of the information that makes up the software and firmware. Snapshots are encrypted and hashed so that any tampering with the snapshot will be immediately detectable. The three snapshots' hash values are compared with each to see if the software has been altered at any stage of the election process.

A reference copy of all software and firmware used by the voting system is obtained by the County Clerk from a third party source such as NIST or from a certified Voting Systems Testing Laboratory. The forensic analysis compares the before and after images listed above to the reference copy and reports on any discrepancies.

The reporting identifies any altered or deleted files, programs, scripts, or other operating components. In the case of a discrepancy, the analysis can recover the information and identify the precise lines of code that were added, altered or deleted.

Not all jurisdictions take this approach. In California, for example, the state requires that a master image be created and that image be reinstalled prior to every election. The master images are created using the trusted build files that are provided to the jurisdiction by the EAC or State of California. The trusted build is the file that is built from the source code that was reviewed and certified.

The decision of how often to create master images are a case-by-case decision, but the broader point remains: the ability to restore from a backup is critical to graceful recovery, and the ability to compare a system to a known good state is critical for identifying problems.

Incident response generally follows a lifecycle of: prepare; detect and analyze; contain, eradicate, and recover; and manage post-incident. Again, it begins with documenting and exercising, but in recovery this includes specific information about the systems and processes that may be impacted, such as knowing the hardware and software comprising specific systems, as well as things such as hashes of critical files—a way to validate whether a file has been tampered with from its last known good state. In preparing for incident recovery, one of the most critical mitigation strategies is to ensure proper backups that are secured separately from the affected systems and networks in advance of a potential incident.

The process of actually recovering starts with understanding the incident. As part of that analysis, decision-makers need to understand the impact of the incident so they can prioritize resources appropriately. Recovery is about getting back to a viable state—in some cases, the priority isn't to directly fix the problem, but rather to work around it to get to the desired outcome without the affected system. This is nothing new in the elections context: when a vote capture device breaks, it may be desirable to fix it, but it may be better at the moment to move to paper ballots so votes can be cast efficiently. The same logic may apply in a cybersecurity context across the elections ecosystem; the most important reaction is often to return to an operational state, even if it's not the optimal state.

Recovery, then, is about getting to the best possible outcome in light of the current circumstances. With proper planning and exercising, officials can avoid the impact of an incident that could prevent successfully executing an election, even when seemingly all has gone wrong.

Attacks such as those that would be directed at an election come with a motivation to impact the election in some way. Nothing serves as a greater disincentive to an attacker than knowing that their target will recover quickly and completely. And little serves to build trust with the public like a plan to achieve an accurate result even if an attack is successful. Just as with other aspects of cybersecurity, by taking the time to prepare before an incident occurs, election officials can actually turn away attackers before they arrive.

Contracting for systems or services

Many organizations use contractors or vendors to provide election system components and services to support elections processes or elections system operations. Election officials should assess the contracted supply chain in addition to support provided internally. In instances where there is contract support, officials should carefully analyze requirements for security and clearly define them in the contract. The government organization that is doing the contracting has the responsibility to assess the security risks for the component or service based on an evaluation of potential threats and security weaknesses or vulnerabilities as well as the probability of occurrence and resulting consequences. Security considerations should be an important consideration in the process of evaluating and selecting a contractor.

If the elections staff is contracting for services that are managed by a contractor or vendor, such as hosting of elections-related software or operations of elections systems, the contract should require that the company providing managed services also provide documentation of their cybersecurity processes and controls, including security metrics that are being collected and monitored. Contractor controls can then be compared to the controls listed in this handbook.

The contract should include a definition of services to be delivered (called a service level agreement or SLA) that includes security controls identified in this handbook. Moreover, a best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits.

For elections system components that are subject to elections system certification requirements, evidence of certification is required. Ideally, there should also be a provision for the contractor to provide security updates to the component over its lifecycle to ensure that vulnerabilities that are discovered are corrected and the component is recertified. For system components or services that are not subject to certification, security requirements will need to align with the particular capabilities or services provided in the contract. Many of the best practices listed in this handbook may be appropriate to include as contract requirements.

In general, the contract should require that the contractor provide a security plan as one of the initial contract deliverables. The security plan should describe how the contractor will meet the security obligations of the contract and specify the security practices and procedures that will be used. Of particular importance in specifying security requirements for contractors will be to address how elections-sensitive information (e.g., ballot layout, voter personal information, vote results) is protected during the execution of the contract and how information records are destroyed.

Additionally, contracts should address the obligations of contracted system operators and public sector clients in regards to identity theft liability, control of and access to public and private data under open records laws, and incident response plans and processes. Where possible, contracts also should specify that vendors transmit network, system, and application logs to the client's security information and event management tools if the client requests. This would allow election officials and their staffs to review and monitor activity instead of being solely reliant on the vendor's capacity for monitoring.

Guidelines for ensuring security of contracted support has been described in the publication ISO/IEC 27002. Specifically, section 15 of the standard describes security issues that should be addressed in dealing with suppliers. The Appendix to this handbook contains a reproduction of this section.

Contracting and technical personnel are encouraged to use this or a similar resource to help identify and assess potential risks as well as responsibilities that will need to be addressed in contract documents and in managing suppliers.

Security best practices

These recommendations are derived from extensive experience understanding the types of vulnerabilities found and attacks experienced across a very wide variety of enterprises, and then translating that into specific and positive steps to mitigate those vulnerabilities and threats. Those recommendations are tailored based on the system and "mission" issues that are unique to elections systems, and the confidence expected for successful outcomes. The process used also examined the various guidelines and specifications used in this sector in order to maintain consistency and minimize overlap.

All of the recommended practices are grouped by class of connectedness (i.e., network connected, indirectly connected, transmission), which was identified as the key factor in assessing security risk. In addition, recommended practices that specifically deal with transmission (electronically or manually) are grouped as a collection for ease of reference.

Network Connected

Network connected components work directly with other devices or systems to achieve their objectives. These connections provide many benefits (e.g., remote diagnostics and management, simple data transfer, rapid updating), but also introduce additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means to accessing and managing the devices, which means organizations must take extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet.

Indirectly Connected

Indirectly connected components are not persistently interconnected with other devices. They do, however, have to exchange information in order to complete their objectives in the election process. While these devices do not carry the same risks associated with being connected to a network or the internet, connecting these components to other devices, either through the use of removable media or direct wired connects, can introduce threats. Mitigating these risks requires a particular set of controls and recommendations when managing the device.

Transmission

In addition to the level of network connectedness, recommendations to address the broader risk of transmission of information across systems are listed separately. These can provide different and sometimes unexpected avenues of attack. These can also involve information transmitted to or from supporting systems that are easy to overlook in terms of security criticality (e.g., the printing of pollbooks, scheduling systems).

Structure of the best practices

Each best practice includes the following information:

- Asset Class (Device, Process, Software, User) — the portion of the overall system to which the practice applies.
- Priority (High, Medium, Low) — from a security perspective (in this handbook, only High and Medium practices have been included).
- Applicable CIS Controls — a cross-reference to the most applicable of the CIS Controls (which can provide a deeper description of this type of practice, and pointers to other information).

We also provide information intended to help decision-makers calibrate the potential challenges of implementation. However, these should be treated as rough guidelines for a "typical" situation – not a rule that can be applied to every election system.

- Potential User Resistance (Yes/No) — Would implementation of the practice be expected to cause resistance or complaints by users and operators of the system? If so, extra care might be needed for rollout or training; and care should be taken so that implementation doesn't encourage the use of risky "work-arounds."
- Upfront Cost (High, Medium, Low) — Does this practice typically require the purchase of new technology, or other significant capital expenditure (High)? Items can be listed as Low when no separate purchase is needed, often because the recommendation can be implemented using existing technology, into the basic configuration of the purchased system, or through operator action.
- Operational Cost (High, Medium, Low) — What are the expected post-purchase costs of this practice? Are there high costs associated with things like supplies (e.g., media, special licensing)?

Summary of connectedness in elections infrastructure components

Part 2 describes the components of a generalized elections system. The end of each subsection classified the different approaches to implementing each component based on the extent to which the component is connected to networks. These connectedness classifications are summarized in Table 1 and form the basis of the best practices. Depending on specific implementation, some of these classifications may vary. However, unless compelling information suggests otherwise, components should be protected at the level indicated.

From Part 2, election officials and others should be able to step through each component to determine the manner (or manners) in which it is implemented in a given election jurisdiction. Once the approach is known, the connectedness classification, summarized here, maps to specific sets of best practices found in the remainder of Part 3.

As noted in Part 2, the components below are a subset that, in our view, reflect the highest risk targets. For digital components not listed below, the analysis methods described in Part 2 can be applied to determine the appropriate correctness class and the associated best practices applicable to that component.

Practitioners can implement these best practices in any order, but we recommend beginning with the high priority best practices.

TABLE 1:

Summary of connectedness for elections infrastructure components

Component		Type within component	Connectedness Class
Voter registration		Master systems and databases	Network connected
	1	Online	Network connected
	2	Paper-based	Not connected
		Transmission of a registration via email or fax	Transmission-based
Pollbooks		e-Pollbook, connects via a wired or wireless network	Network connected
		e-Pollbook, connects via a physical media connection or removable media	Indirectly connected
		Transmission of data for printing via a network connection, website portal, or email	Transmission-based
		Transmission of data for printing via a wired media connection or removable media	Transmission-based
EMS	1	Unless definitively known to have no network capabilities	Network connected
	2	If known definitively to have no network capabilities	Indirectly connected
Vote capture		Vote capture device transmits data for any reason—or if the functionality is enabled regardless of whether it is used	Network connected
	1	Voter marked and hand counted paper balloting	Not connected
	2	Voter marked paper balloting with scanning	Indirectly connected
	3	Electronic voting with paper ballot output	Indirectly connected
	4	Electronic voting with paper record	Indirectly connected
	5	Electronic voting with no paper record	Indirectly connected
	6	Electronic receipt and delivery of ballots conducted remotely	Transmission-based
Vote tabulation	1	Connects via a wired or wireless connection	Network connected
	2	All others	Indirectly connected
Election night reporting	1	If receiving tabulated votes via a wired or wireless connection	Network connected
	2	If receiving tabulated votes via a wired media connection or removable media	Indirectly connected
Election night publishing	1	All	Network connected

Best Practices

The following best practices address the risks identified elsewhere in this handbook. References to resources are listed in the Appendix.

Connectedness Class	Priority
Network Connected	**High**

1 Whitelist which IPs can access the device

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources

CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

2 Regularly scan the network to ensure only authorized devices are connected

Applicable CIS Controls

#1.1: Automated Asset Inventory Tool

Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

#12.8: Periodically Scan For Back-channel Connections To The Internet

Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources

Automated tools should be available to actively scan the internal environment, while DHS and MS-ISAC services can assist organizations with scanning their externally facing assets.

continued:

Connectedness Class
Network Connected

Priority
High

3 Limit the devices that are on the same subnet to only those devices required

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class

Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources

NIST guidance is available to help the technical team determine how to appropriately segregate assets and permit access to only those devices or systems requiring access: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

4 Only utilize approved and managed USB devices with appropriate device encryption and device authentication

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources

CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

continued:

Connectedness Class
Network Connected

Priority
High

5 Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (Bluetooth, WiFi, radio, microwave, satellite, etc.) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth and WiFi), unless such access is required and risk acceptance is formally documented.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Microsoft guidance on how to disable Bluetooth: https://technet.microsoft.com/en-us/library/dd252791.aspx.

6 Ensure the system is segregated from other independent election systems and non-election supporting systems

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the type of information and the sensitivity of the information processes and stored. Use virtual LANS (VLANS) to protect and isolate information and processing with different protection requirements with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	High	Medium

Resources
While this is an often overlooked control and can require architectural redesigns, this is an important control to pursue. NIST guidance on boundary protection: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

continued:

Connectedness Class
Network Connected

Priority
High

7 Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on Internet and extranet DMZ systems

Applicable CIS Controls

#12.2: Record At Least Packet Header Information On DMZ Networks

On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources

The Albert device is part of the MS-ISAC offering: https://www.cisecurity.org/ms-isac/services/albert/. There are a number of commercially-available options, such as: https://securityonion.net/.

8 If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)

Applicable CIS Controls

#15.5: Protect All Wireless Traffic with AES and WPA2

Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources

NIST guidance on how to implement secure wireless networks: https://www.nist.gov/publications/guidelines-securing-wireless-local-area-networks-wlans.

9 Use trusted certificates for any publicly-facing website

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources

Vendor recommendation on deploying certificates with the system. Also, test to verify SSL certificate configuration, with products such as with Qualys: https://www.ssllabs.com/ssltest/.

continued:

Connectedness Class
Network Connected

Priority
High

10 Ensure logs are securely archived

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security: https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

11 On a regular basis, review logs to identify anomalies or abnormal events

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

12 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls
#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft guidance on digital signatures: https://technet.microsoft.com/en-us/library/cc962021.aspx.

13 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

continued:

Connectedness Class
Network Connected

Priority
High

14 Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

15 Ensure acceptance testing is done when receiving or installing new/updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

16 Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

continued:

Connectedness Class
Network Connected

Priority
High

17 Deploy application whitelisting

Applicable CIS Controls

# 2.2: Deploy Application Whitelisting

Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Low

Resources

NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

18 Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards

Applicable CIS Controls

#3.1: Establish Standard Secure Configurations For OS And Software

Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

#18.7: Use Standard Database Hardening Templates

For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	High	Low

Resources

CIS Benchmarks provide hardened configurations for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/. In addition, NIST provides additional recommendations for baselines https://nvd.nist.gov/800-53/Rev4/control/CM-2. Some vendor products may require tailoring to work with benchmark configured systems. Deviations from the benchmark should be documented.

continued:

Connectedness Class
Network Connected

Priority
High

19 Regularly run a SCAP-compliant vulnerability scanner

Applicable CIS Controls

#4.1: Weekly Automated Vulnerability Scanning

Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Medium

Resources

Principal cost beyond the purchase of the tool is the adjudication and remediation of the findings. SCAP validated tools can be found at: https://nvd.nist.gov/scap/validated-tools and there are a number of other commercially available tools.

20 Utilize EAC certified or equivalent software and hardware products where applicable

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Medium

Resources

Guidance from EAC about their vendor certification process: https://www.eac.gov/voting-equipment/frequently-asked-questions/.

21 Store secure baseline configuration on hardened offline system and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely

Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Network Connected

Priority
High

22 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

23 Maintain detailed maintenance record of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST guidance: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

24 Require the use of multi-factor authentication

Applicable CIS Controls

#5.6: Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

#12.6: Require Two-factor Authentication For Remote Login
Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

#16.11: Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	High	Medium

Resources
Vendor specific. NIST guidance on authentication: https://pages.nist.gov/800-63-3/sp800-63b.html.

continued:

Connectedness Class
Network Connected

Priority
High

25 Require users to use strong passwords (14 character passphrases) if multi-factor authentication is not available

Applicable CIS Controls

#5.7: User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

#16.12: Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Vendor specific. CIS Benchmarks details how this can be implemented for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/.

26 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls

#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class	Priority
Network Connected	**Medium**

27 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources

NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

28 Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources

Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

29 Maintain an inventory of assets that should be on the same subnet as the election system component

Applicable CIS Controls

#1.4: Asset Inventory Accounts For All Devices

Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources

NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Network Connected

Priority
Medium

30 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources

Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

31 Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Medium	Low

32 Limit the use of personally identifiable information. When it is required, ensure that it is properly secured and staff with access are properly trained on how to handle it.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

Resources

Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

33 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Network Connected

Priority
Medium

34 Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities

Applicable CIS Controls

#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

35 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

36 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

37 Work with vendors to establish and follow hardening guidance for their applications

Applicable CIS Controls

#3.1: Establish Standard Secure Configurations For OS And Software

Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources

Vendors will typically provide recommendations on how to securely deploy and manage their systems.

continued:

Connectedness Class
Network Connected

Priority
Medium

38 Ensure logging is enabled on the system

Applicable CIS Controls

#6.2: Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Medium

Resources

Work with Vendor to identify logging capabilities. CIS-CAT can check this configuration item for consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. CIS Benchmarks provides logging recommendations for major platforms: https://www.cisecurity.org/cis-benchmarks/.

39 Use automated tools to assist in log management and where possible ensure logs are sent to a remote system

Applicable CIS Controls

#6.6: Deploy A SIEM or Log Analysis Tools For Aggregation And Correlation/Analysis

Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	High	High

Resources

A variety of tools that have various capabilities and costs as well as the effort and rigor of the review and retention of the logs which will have varying costs. Windows Event Subscription Guide: https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

40 Where feasible, utilize anti-malware software with centralized reporting

Applicable CIS Controls

# 8.1: Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
Vendor specific.

41 Ensure only required ports are open on the system through regular port scans

Applicable CIS Controls

#9.3: Perform Regular Automated Port Scanning
Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

#9.1: Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Checkable by CIS-CAT and other SCAP-validated tools (https://nvd.nist.gov/scap/validated-tools), and other network scanning tools such as NMAP: https://nmap.org.

continued:

Connectedness Class
Network Connected

Priority
Medium

42 Where feasible, implement host-based firewalls or port filtering tools

Applicable CIS Controls

#9.2: Leverage Host-based Firewalls

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Medium

Resources

If host-based, can be verified by CIS-CAT: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on implementing firewalls: https://technet.microsoft.com/en-us/library/cc772353(v=ws.10).aspx.

43 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

44 Ensure vendors distribute software packages and updates using secure protocols

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources

Work with the election software vendors.

continued:

Connectedness Class
Network Connected

Priority
Medium

45 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

46 All remote connections to the system will use secure protocols (TLS, IPSEC)

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as, TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

CIS-CAT can identify whether secure protocols are configured consumer grade operating system: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

47 Users will use unique user IDs

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

48 Use a dedicated machine for administrative tasks to separate day to day functions from other security critical functions. (For some components this may not be practical to implement.)

Applicable CIS Controls

#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Low

Resources
For some components this may not be practical to implement.

49 Ensure that user activity is logged and monitored for abnormal activities

Applicable CIS Controls

#16.10: Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Medium

Resources
CIS-CAT can identify these at the consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. It is desirable to have a log aggregation or SIEM system in place to aggregate and analyze logs for abnormal behaviors.

continued:

Connectedness Class
Network Connected

Priority
Medium

50 Regularly review all accounts and disable any account that can't be associated with a process or owner

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

51 Establish a process for revoking system access immediately upon termination of employee or contractor

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

Resources on the process potentially involved with termination process NIST: https://nvd.nist.gov/800-53/Rev4/control/PS-4.

continued:

Connectedness Class
Network Connected

Priority
Medium

52 Ensure that user credentials are encrypted or hashed on all platforms

Applicable CIS Controls

#16.14: Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

CIS-CAT can identify this configuration on consumer grade operating systems and applications, work with vendor to verify: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

53 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls

#16.5: Configure screen locks on systems to limit access to unattended workstations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources

Work with dedicated purpose election system vendors to verify their products. CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

54 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Connectedness Class	Priority
Indirectly Connected	**High**

55 For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging

Applicable CIS Controls

#13.5: Disable Write Capabilities To USB Devices

If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Medium	Low

Resources

Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

56 Disable wireless peripheral access of devices

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (i.e. Bluetooth) Unless Required

Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Low	Low

Resources

Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

continued:

Connectedness Class
Indirectly Connected

Priority
High

57 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC Guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

58 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

59 Ensure staff is properly trained for reconciliation procedures for the pollbooks to the voting systems and reconcile every polling place and voter record in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

60 Store secure baseline configurations on hardened offline systems and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Indirectly Connected

Priority
High

61 Work with the vendor to deploy application whitelisting

Applicable CIS Controls

#2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	Yes	Medium	Low

Resources

NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

62 Utilize the most up-to-date and certified version of vendor software

Applicable CIS Controls

#4.5: Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

#18.1: Use Only Vendor-supported Software
For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low Medium	

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Indirectly Connected

Priority
High

63 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

64 Only use the devices for election related activities

Applicable CIS Controls

#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Medium	Low

Resources
Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

65 Maintain detailed maintenance records of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

continued:

Connectedness Class
Indirectly Connected

Priority
High

66 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls

#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Indirectly Connected

Priority
Medium

67 Utilize tamper evident seals on all external ports that are not required for use

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

68 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

69 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

70 Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

71 Ensure acceptance testing is done when receiving or installing new or updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

72 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

73 Identify and maintain information on network service providers and third-party companies' contacts with a role in supporting election activities

Applicable CIS Controls

#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

74 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

75 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

76 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	Medium	No	Medium	Low

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

77 Ensure the use of unique user IDs

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

78 Ensure individuals are only given access to the devices they need for their job

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

How to implement least privilege within an organization according to NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-6.

79 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

80 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls

#16.5: Configure screen locks on systems to limit access to unattended workstations

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Work with special purpose election system vendors to verify their products.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

81 Regularly review all authorized individuals and disable any account that can’t be associated with a process or owner

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Medium	Medium

Resources

Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

82 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Connectedness Class
Transmission

Priority
High

83 Use secure protocols for all remote connections to the system (TLS, IPSEC)

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that Table5 not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Low	Low

Resources

CIS-CAT can identify whether secure protocols are configured for common operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

continued:

Connectedness Class
Transmission

Priority
High

84 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls

#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Medium	Medium

Resources

Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security:
https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Connectedness Class
Transmission

Priority
Medium

85 Ensure the use of bi-directional authentication to establish trust between the sender and receiver

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Low

86 For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources

Check to see if vendors have this information as part of their product offerings. Additionally see information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

continued:

Connectedness Class
Transmission

Priority
Medium

87 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

88 Track all hardware assets used for transferring data throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

Appendix:
References and Resources

This section provides references to the resources cited in this handbook, including Section 15 of ISO/IEC 27002, which we reproduce with permission from ISO.

In addition, the website for this handbook, https://www.cisecurity.org/elections-resources/, has additional resources, such as more best practices from local elections officials, that may be useful for readers.

CIS resources

Under the sponsorship of the U.S. Department of Homeland Security, CIS offers a number of services to U.S. State, Local, Tribal, and Territorial (SLTT) government entities at no charge. Specifically, SLTT entities can take advantage of the following resources:

- Become members of the MS-ISAC (Multi-State Information Sharing and Analysis Center) for coordination of cybersecurity readiness and response (https://www.cisecurity.org/ms-isac/)
- Access the CIS Controls—20 foundational and advanced cybersecurity actions that can eliminate the most common attacks (https://www.cisecurity.org/controls/)
- Access the CIS Benchmarks—a set of configuration guidelines to safeguard operating systems, software, and networks (https://www.cisecurity.org/cis-benchmarks/)
- Obtain membership to CIS SecureSuite—a set of integrated cybersecurity resources to help start secure and stay secure (https://www.cisecurity.org/cis-securesuite/)
- Use CIS-CAT Pro, to quickly compare and report on the configuration of systems against CIS Benchmark recommendations (https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/)
- Purchase through CIS CyberMarket—a program to improve cybersecurity through cost-effective group procurement (https://www.cisecurity.org/services/cis-cybermarket/)
- Access CIS WorkBench—a community website that serves as a hub for tech professionals to network, collaborate, discuss technical concepts, and download CIS resources (https://www.cisecurity.org/introducing-cis-workbench/)

CIS has gathered additional resources specific to the elections community at https://www.cisecurity.org/elections-resources/. In addition to an electronic version of the handbook, the site includes additional examples of best practices in use in state and local jurisdictions, as well as other resources that may be useful to organizations implementing the best practices.

CIS also provides support beyond that funded by DHS (called "partner paid" services) if needed by SLTT organizations. Examples of partner paid services include additional Albert sensors and security monitoring services as well as tailored cybersecurity support.

Individuals working for any State, Local, Tribal, or Territorial government should contact CIS at info@msisac.org to find out what's best for their organization. Commercial entities, such as vendors of election systems and service providers, are also welcomed to access many of these services, in many cases free of charge.

Other resources referenced in this handbook

Department of Homeland Security. https://www.dhs.gov/.

Designation of chief State election official, 52 USC 20509 (2014). Accessed at https://www.gpo.gov/fdsys/pkg/USCODE-2014-title52/html/USCODE-2014-title52-subtitleII-chap205-sec20509.htm.

Election Assistance Commission. https://www.eac.gov/.

Election Assistance Commission. (2015). *Election Assistance Commission Statutory Overview: 2014*. Retrieved from https://www.eac.gov/assets/1/1/2014_Statutory_Overview_Final-2015-03-09.pdf.

Financial Sector Information Sharing and Analysis Center. https://fsisac.com/.

Harris, Joseph P. (1934). *Election Administration in the United States.* Brookings Institution Press, Washington D.C. Retrieved from https://www.nist.gov/itl/election-administration-united-states-1934-joseph-p-harris-phd.

International Organization for Standardization. (2011). *Information technology—Security techniques—Information security risk management.* ISO/IEC 27005:2011. Available at https://www.iso.org/standard/56742.html.

International Organization for Standardization. (2013). *Information technology—Security techniques—Code of practice for information security controls.* ISO/IEC 27002:2013. Available at https://www.iso.org/standard/54533.html.

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments.* NIST SP800-30. Available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Available at https://www.nist.gov/cyberframework.

"Principles and Best Practices for Post-Election Audits." Edited by Mark Lindeman et al., Principles and Best Practices for Post-Election Audits, 1 Sept. 2008, www.electionaudits.org/principles.html.

Volunteer Voting System Guidelines, version 1.1. (2015). *Elections Assistance Commission.* Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

Summary of resources referenced in this handbook's best practices

Cisco Systems, Inc. "Configuring IP Access Lists." *Cisco,* 5 June 2017, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

Election Assistance Commission. "Election Management Guidelines." *U.S. Election Assistance Commission (EAC),* https://www.eac.gov/election-officials/election-management-guidelines/.

Fyodor. "Nmap." *Nmap: the Network Mapper - Free Security Scanner,* 1 Aug. 2017, https://nmap.org/.

General Services Administration. "GSA Forms Library." *Basic National Agency Check Criminal History,* 17 Aug. 2017, https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

Johnston, Roger G. "Tamper-Indicating Seals: Practices, Problems, and Standards." *World Customs Organization Security Meeting,* 11 Feb. 2003, http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

Microsoft Corp, Inc. "Digital signatures." *Microsoft TechNet,* https://technet.microsoft.com/en-us/library/cc962021.aspx.

Microsoft Corp, Inc. "Disabling Bluetooth and Infrared Beaming." *Microsoft TechNet,* 9 Feb. 2009, https://technet.microsoft.com/en-us/library/dd252791.aspx.

Microsoft Corp, Inc. "Event Subscriptions." *Windows Server 2008 R2 and Windows Server 2008,* 22 Feb. 2013, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "How to Set Event Log Security Locally or by Using Group Policy." *How to Set Event Log Security Locally or by Using Group Policy,* 7 Jan. 2017, https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Microsoft Corp, Inc. "Lesson 1: Managing User Accounts." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Microsoft Corp, Inc. "Managing Windows Firewall with Advanced Security." *Windows Server 2008 R2 and Windows Server 2008,* 2 July 2012, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "Securing Remote Access." *Microsoft Developer Network*, https://msdn.microsoft.com/en-us/library/cc875831.aspx.

National Institute of Standards and Technology. (2012). *Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks.* NIST SP 800-153. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf.

National Institute of Standards and Technology. (2013). *Special Publication 800-35 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53r4. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

National Institute of Standards and Technology. (2015). *Special Publication 800-167: Guide to Application Whitelisting.* NIST SP 800-167. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

National Institute of Standards and Technology. (2017). *Special Publication 800-63B: Digital Identity Guidelines Authentication and Lifecycle Management.* NIST SP 800-63B. Available at https://pages.nist.gov/800-63-3/sp800-63b.html.

National Institute of Standards and Technology. *National Vulnerability Database.* Available at https://nvd.nist.gov.

Onion Solutions, LLC. "Security Onion." *Security Onion,* https://securityonion.net/.

Qualys, Inc. "SSL Server Test." *SSL Server Test,* (2018), https://www.ssllabs.com/ssltest/.

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls

15 Supplier relationships

15.1 Information security in supplier relationships

15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

b) a standardised process and lifecycle for managing supplier relationships;

c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;
e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;
f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;
g) types of obligations applicable to suppliers to protect the organization's information;
h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;
i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;
j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;
k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information
Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control
All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance
Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;
b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
e) rules of acceptable use of information, including unacceptable use if necessary;
f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;
g) information security policies relevant to the specific contract;
h) incident management requirements and procedures (especially notification and collaboration during incident remediation);
i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures; relevant regulations for sub-contracting, including the controls that need to be implemented;
j) relevant agreement partners, including a contact person for information security issues;
k) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;
l) right to audit the supplier processes and controls related to the agreement;
m) defect resolution and conflict resolution processes;
n) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
o) supplier's obligations to comply with the organization's security requirements.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers). The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;
b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;
c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain
d) if these products include components purchased from other suppliers;

e) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;
f) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside
g) of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
h) obtaining assurance that critical components and their origin can be traced throughout the supply chain; obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
i) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;
j) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management

15.2.1 Monitoring and review of supplier services

Control

Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;
b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
c) conduct audits of suppliers, in conjunction with review of independent auditor’s reports, if available, and follow-up on issues identified;
d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
f) resolve and manage any identified problems;
g) review information security aspects of the supplier's relationships with its own suppliers;
h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

Implementation guidance
The following aspects should be taken into consideration:

a) changes to supplier agreements;
b) changes made by the organization to implement:
    1) enhancements to the current services offered;
    2) development of any new applications and systems;
    3) modifications or updates of the organization's policies and procedures;
    4) new or changed controls to resolve information security incidents and to improve security;
c) changes in supplier services to implement:
    1) changes and enhancement to networks;
    2) use of new technologies;
    3) adoption of new products or newer versions/releases;
    4) new development tools and environments;
    5) changes to physical location of service facilities;
    6) change of suppliers;
    7) sub-contracting to another supplier.

Department of Homeland Security (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC)

ISAC Pilot for Election Infrastructure

October 2017

Homeland Security

ISAC PILOT
for Election Infrastructure

MS-ISAC
Multi-State Information
Sharing & Analysis Center

Project Team Members

DHS

- Rob Gatlin, Program Manager
- Donna Beach, ISAC Pilot Leader for Elections Infrastructure

COLORADO

- Judd Choate, State Election Director
- Trevor Timmons, CIO
  - Hilary Rudy, Deputy Director of Elections Division
  - Rich Schliep, CISO

INDIANA

- Connie Lawson, Secretary of State
  - Brandon Clifton, Deputy Secretary of State
- Thomas Vessely, Director of IT
- Patrick Glover, Assistant Director of IT
  - Jerry Bonnet, General Counsel

NEW JERSEY

- Robert Giles, Director, Division of Elections
- Kevin Kearns, Bureau Chief, Cybersecurity Governance, Risk, and Compliance
- James Simmons, Vice President, Technology & Operations
  - Vasiliy Bessonov
  - Michael DiSimoni
  - Michael Geraghty

MS-ISAC

- Ben Spear, MS-ISAC Project Leader
- Kateri Gill, MS-ISAC Stakeholder Engagement

TEXAS

- Keith Ingram, Elections Division Director
- Scott Brandt, IT Division Director
- Marlin Craig, Information Security Officer
- Michael Winn, Travis County Director of Elections

UTAH

- Justin Lee, Director of Elections
- Mark Mitchell, IT Director
- Phil Bates, State Information Security Director
- Ricky Hatch, Weber County Clerk/Auditor
- Matt Mortensen, Weber County IT Security Specialist

VIRGINIA

- Edgardo Cortes, Elections Commissioner
- Matt Davis, CIO
- Michael Watson, CISO
  - Elizabeth Howard, Elections Deputy Commissioner

WASHINGTON

- Lori Augino, Director of Elections
- Michael Huntley, CIO
- Harold Stoehr, CISO

Homeland Security

Project Progress

Oct 12
- Initiated HSA Monthly Update

Oct 18
- Initiated Newsletter Distribution

Oct 27
- Initiated Election Specific Cyber Alerts

Oct 31
- Initiated MS-ISAC Monthly Member Call

Nov 3
- Initiated National Webcast
- Initiated Vulnerability Management Profiles

Nov 9
- Initiated Monthly Situational Awareness Report

Nov 13
- Initiated Alerting of IPs and Domains

Nov 20
- Initiated Weekly Elections Cyber News Alert

Nov 21
- Onboarding Complete

Operational Updates

MS-ISAC
Multi-State Information
Sharing & Analysis Center

Weekly Elections Cyber News Alert

- Purpose: Weekly news summary of open-source reporting on election cybersecurity risks and best practices.
- Design
  - Title – Source – Date
  - Summary
  - Analysis
  - Source Link
- Topics
  - Cybersecurity risk landscape for Elections Infrastructure
  - Legislative action
  - Best practices
  - General technology/cybersecurity awareness with elections link/impact
- Feedback

Homeland
Security

Operational Updates

Elections Cyber Alert Modifications

- Rearranged Sections
  - Executive Overview
  - User Recommendations
  - Technical Description
  - Technical Indicators
  - Technical Recommendations

Albert Monitoring

- Existing Albert Sensors:
  - Utah
  - Virginia
- Albert sensor Deployment:
  - Colorado
  - Indiana
  - New Jersey
  - Texas
  - Washington

Operational Updates

Separation of Technical and Election-Specific Alerts

- Milestone Date: Q2 2018
- Option to receive only products of your choice
  - Advisories
  - Cyber Alerts
  - Election-Specific Cyber Alerts
  - Intel Products
  - Situational Awareness Report
  - Email Notifications

Feedback Survey

- Evaluates objectives and success criteria
  - Customer Service
  - Overall Membership
  - Products and Services provided

- Tool to measure the progress and satisfaction over the course of the pilot
- Frequency: 50, 80 and 110 days

Pilot Duration

60 Day Deliverables

- Election-specific products
  - Election-specific Cyber Alerts
  - Weekly Cyber News
- Traditional MS-ISAC products
  - Advisories
  - Weekly Malicious IPs and Domains
  - Situational Awareness Report
  - HSA Cyber Monthly Update
  - Newsletter
  - MS-ISAC Monthly Member Call
  - Vulnerability Management Program (VMP) Report
- Information Sharing Tools
  - Machine-to-Machine Cyber Indicator Sharing
  - HSIN Portal Access
- Albert Deployment
  - Albert sensors ordered for pilot states
  - Albert notification forwarding for states with existing sensors
- Formalized notification process

Pilot Duration

90 Day Deliverables

- Election-specific products
  - Monthly Analyst-to-Analyst Exchange
  - Distribution extended to registered Elections community (20 states)
- Traditional MS-ISAC products
  - Intelligence products
- Albert deployment
  - Albert sensor delivery

120 Day Deliverables

- Election-specific products
  - Outline - Elections Fusion Analysis Report
- Albert deployment
  - Albert sensors online
  - Albert notifications

Services by Request

- Computer Emergency Response Team (CERT)
- Malicious Code Analysis Platform (MCAP)

Project Communications

Email DHS SLTT Project Team at:
SLTTCyber@HQ.DHS.GOV

Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)

Common Cyber Security Language

August 2018

Common Cyber Security Language

Term	Definition
Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
Accessibility	Information is available and easily usable (formatted for convenient and immediate use).
Accuracy	The closeness between an estimated result and the (unknown) true value.
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
Automatic Train Protection (ATP)	A wayside and/or on-board train system to apply emergency brakes if a signal is missed by the train operator.
Automatic Train Supervision (ATS)	Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.
Black-box	A device that records information, which cannot be changed or manipulated in any manner. The information recorded is used for forensic purposes. It is used in the same sense of an aviation flight recorder.
CJIS Security Policy	The Criminal Justice Information Services (CJIS) Security Policy provides appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The policy also provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.
Coherence	The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, which are similar.
Commercial-off-the-Shelf (COTS)	Products that are readily available commercially and may be used “as is.”
Communications-based Train Control (CBTC)	A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the “moving block” principle for safe train separation rather than fixed blocks with track circuits.
Comparability	The degree to which data can be compared over time and domain.
Configuration Management	A practice and process of handling hardware, software and firmware changes systematically so that a device or system maintains its integrity over time.
Consequence	The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society.
Countermeasure	Action, measure, or device intended to reduce an identified risk.
Critical infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Critical Infrastructure Owners and Operators	Those entities responsible for day-to-day operation and investment of a particular-lar critical infrastructure entity. (Source: Adapted from the 2009 NIPP).
Critical Infrastructure Partner	Governmental entities, public and private sector owners and opera-tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation’s critical infrastructure.
Criticality	Importance to a mission or function, or continuity of operations.
Cryptography	A way to encode (hide) information such that the sender intends that only the recipient should understand the message.
Cyber Incident	An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Cyber System	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, and access control systems.

Cybersecurity	The full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
Cybersecurity (USCG-Specific)	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.
Cyclic Redundancy Check (CRC)	An error detection code used in digital networks to detect accidental changes in data during transmission or storage.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Deterrent	Measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety.
Electronic Security Perimeter (ESP)	Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate it from other zones.
Emergency Cutoff (blue light) system	A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.
Enterprise Risk Management	Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.
Enterprise Zone	The zone of a transit agency that handles its routine internal business processes and other non-operational; non-fire, life-safety; and non-safety-critical information.
Evaluation	Process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives.
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity frame-work; and promote and incentivize the adoption of strong cybersecurity practices.
Fail-safe	A device that fails in a manner that protects the safety of personnel and equipment.
FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Fiber-optic Strand	A portion of a cable in a fiber-optic network. Each strand carries information unique to it and is isolated from all the other strands.
Fire Life-Safety Security Zone (FLSZ)	A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Human-machine Interface (HMI)	The control interface between humans and machines.
Incident	An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber attacks, cyber failure/accident, and other occurrences requiring an emergency response.
Information sharing	The process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty.
Inputs	Resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials.

Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions.
Intrusion	An unauthorized act of bypassing the security mechanisms of a network or information system.
IPSec	A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.
ISO 27001	A standard created by the International Standards Organization (ISO) to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)".
Loss of control	Sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses).
Malware	Short for malicious software. Software created and used by people, usually with bad intentions to disrupt computer operations or obtain, without consent, confidential information.
Man-in-the-middle (MitM)	A type of cyber-attack where an interloper inserts him- or herself in-between two communicating devices, without either side being aware of the interloper.
Mitigation	Capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
National Cyber Investigative Joint Task Force	The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from Federal agencies, including DHS, and from State, local, and international law enforcement partners.
National Cybersecurity and Communications Integration Center	The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents.
Network Resilience	The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.
Operationally Critical Security Zone (OCSZ)	A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.
Operations Control Center	A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.
Outcomes	Events, occurrences or changes in condition that indicate programmatic progress, brought about at least in part through outputs.
Outputs	Completed or delivered products or services generated through inputs.
Patch Management	A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, etc.
Performance management	The use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services.
Performance measurement	Regular measurement of the results (outcomes) and efficiency of services or programs.
PIV-I	PIV Interoperable (PIV-I) cards are smartcards issued by Non-Federal Issuers that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Department or Agency.
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.
Processes	The steps that turn inputs into outputs.
Programmable Logic Controller (PLC)	An industrial computer used for automation of mechanical processes.

Recommended Practice	An APTA Recommended Practice represents a common viewpoint of those parties concerned with its provisions. The application of a Recommended Practice is voluntary.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Recovery	Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.
Recovery	The activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.
Redundancy	Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.
Regional	Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location.
Relevance	The degree to which the product meets user needs for both coverage and content.
Residual Risk	Risk that remains after risk management measures have been implemented.
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.
Risk Assessment	Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
Risk Avoidance	Strategies or measures taken that effectively remove exposure to a risk.
Risk Communication	Exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
Safety Critical Security Zone	The zone that contains vital signaling, interlocking and ATP within rail transit.
Safety Critical Security Zone (SCSZ)	The zone that contains vital signaling, interlocking and ATP within rail transit.
SCADA	A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.
Secure Hash Algorithm (SHA):	A family of cryptographic hash functions used to calculate a unique sum for a digital file to be used to check for later file modifications.
SSAE 16	Statement on Standards for Attestation Engagements (SSAE) 16 reporting can help service organizations comply with Sarbanes Oxley's requirement to show effective internal controls covering financial reporting.
SSI	Sensitive Security Information (SSI) is a specific category of sensitive but unclassified (SBU) information that is governed by Federal law. SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. At TSA, the goal is to release as much information as possible publicly without compromising security.
STRIDE	Defines a Microsoft method to classify computer security threats. The acronym stands for Spoofing of an id, Tampering with data, Repudiation, Information disclosure (breach), Denial of service, and Elevation of privilege.
System	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.
Threat	A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Timeliness	Information is current (it should be released as close as possible to the period to which the information refers).
Track Circuit	An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.
Transportation Security Incident	A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. In this paragraph, the term "economic disruption" does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employee-employer dispute.
Trusted (network)	Network of an organization that is within the organization’s ability to control or manage. Further, it is known that the network’s integrity is intact and that no intruder is present.
Unauthorized Access	Any access to an information system or network that violates the owner or operator's stated security policy.
Uncertainty	The state of being not known, indeterminate, questionable, variable.
Vector (for cyber-attack)	The path an attacker takes to attack a network.
Virtual Private Network	A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet.
Vital Signaling	The portion of a railway signaling network that contains vital equipment.
Vital-programmable Logic Controller (vital-PLC)	A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.
Vulnerability	A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
White-listing	Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.
Wi-Fi	In the broadest sense, all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

A Note on the Common Cyber Language: The resources on this page have been submitted by the Common Language Initiative Team, a subcommittee of the Transportation Systems Sector Cyber Working Group (TSSCWG). While they represent a small fraction of the available documents and tools available to the Transportation Systems Sector, and the Cyber Security Community as a whole, they stand out to the individuals/modes of transportation that submitted them. Over time, this living document will be revisited to add/remove terminology and/or references to ensure its relevance. For questions or recommendations on the Common Language, please email CyberSecurity@tsa.dhs.gov.

Additional Resources

Website/Document Name	Cyber Security Language Resources
2013-2023 Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy	**http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf**
American Institute of Certified Public Accountants (AICPA)	http://ssae16.com/SSAE16_overview.html
Committee on National Security Systems- CNSS Instruction No. 4009- National Information Assurance (IA) Glossary	http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf
Cyber Risk and Insurance Forum (CRIF) Cyber Security Glossary	http://www.cyberriskinsuranceforum.com/content/cyber-security-glossary
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
Federal CIO Council	https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf
General Services Administration (GSA)	http://www.fedramp.gov/
Glossary- McAfee for Consumer	http://home.mcafee.com/virusinfo/glossary?ctst=1#A
Glossary of Key Information Security Terms	http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Glossary- Symantec Enterprise	http://www.symantec.com/security_response/glossary/
Honeywell Industrial Cyber Security Glossary	https://www.honeywellprocess.com/en-US/online_campaigns/IndustrialCyberSecurity/Pages/glossary.html
International Standards Organization (ISO)	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
ISACA- Cybersecurity Fundamentals Glossary	http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Joint Publication 3-12®- Cyberspace Operations	http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)- Cyber Definitions	https://ccdcoe.org/cyber-definitions.html

NICCS- A Glossary of Common Cybersecurity Terminology	http://niccs.us-cert.gov/glossary
NIPP 2013- Partnering for Critical Infrastructure Security and Resilience	http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf
NIST- Framework for Improving Critical Infrastructure Cybersecurity	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
PCI Security Standards Council	https://www.pcisecuritystandards.org/security_standards/
Presidential Policy Directive- Critical Infrastructure Security and Resilience (PPD-21)	https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Presidential Policy Directive- National Preparedness (PPD-8)	http://www.dhs.gov/presidential-policy-directive-8-national-preparedness
Radio Technical Commission for Aeronautics (RTCA)- SC-216 Aeronautical Systems Security	http://www.rtca.org/content.asp?pl=108&sl=33&contentid=82
Risk Steering Committee- DHS Risk Lexicon	http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
Roadmap to Secure Control Systems in the Transportation Sector	https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf
SANS- Glossary of Security Terms	https://www.sans.org/security-resources/glossary-of-terms/
The University of Texas at Austin- Cyber Security Glossary Terms	http://www.utexas.edu/its/glossary/secure
The University of Texas at Austin- Identity and Cybersecurity Terms	https://identity.utexas.edu/everyone/glossary-of-identity-and-cybersecurity-terms
Transportation Security Administration	https://www.tsa.gov/sites/default/files/assets/pdf/ssi/ssi_reg_5-18-04.pdf
United States Coast Guard Cyber Strategy	https://homeport.uscg.mil/cgi-bin/st/portal/uscg_docs/MyCG/Editorial/20150706/CG_Cyber_Strategy_Final.pdf?id=0f151e6b1eb70b5aa8e5776e0e07d0c2c353f8e4&user_id=087c7ada72ee5d101ec55060bf4af6ce

Online Communities

Organization	Website
NIEM- National Information Exchange Model <REGISTRATION REQUIRED>	**https://www.niem.gov/communities/emc/Pages/emerging-communities.aspx**
NIEM- National Information Exchange Model	https://www.niem.gov/communities/emc/cyber/Pages/about-cyber.aspx

Election Assistance Commission (EAC)
Glossary of Common Cybersecurity Terms

August 2018

Glossary
Common Cybersecurity Terminology

Access
Ability to make use of any information system (IS) resource.

Source: CNSSI 4009-2015

Access control
The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Source: FIPS 201-2

Access control mechanism
Security safeguards designed to detect and deny unauthorized access and permit authorized access to an information system.

Source: CNSSI 4009-2015

Advanced Persistent Threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Source: NIST SP 800-39

Adversary
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Source: NIST SP 800-30 Rev. 1 (DHS Risk Lexicon)

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e. data is transferred through the interface only manually, under human control).

Source: CNSSI 4009-2015

Alert
Notification that a specific attack has been directed at an organization's information systems.

Source: CNSSI 4009

Antivirus software
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Source: NIST SP 800-94, NIST SP 800-83 Rev. 1

Asset
A major application, general support system, high impact program, physical plan, mission critical system, personnel, equipment, or a logically related group of systems.

Source: CNSSI 4009-2015

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Source: NIST SP 800-82 Rev. 2 (CNSSI 4009)

Attack signature
A specific sequence of events indicative of an unauthorized access attempt.

Source: NIST SP 800-12

Attacker
A party who acts with malicious intent to compromise an information system.

Source: NIST SP 800- 63 Rev 2

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Source: NIST SP 800-32 (CNSSI 4009)

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Source: NIST SP 800-53 Rev. 4

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: CNSSI 4009 (FIPS 200, NIST SP 800-27 Rev. A)

Authority

The aggregate of people, procedures, documentation, hardware, and/or software necessary to authorize and enable security-relevant functions.

Source: NIST SP 800-57 Part 2

Availability

Timely, reliable access to data and information services for authorized users.

Source: CNSSI 4009-2015, NIST SP 800-70 Rev 2

Backups

A copy of files and programs made to facilitate recovery if necessary.

Source: NIST SP 800-34 Rev. 1

Black-box testing

A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Source: CNSSI 4009-2015, IST SP 800-53A Rev 4. (adapted)

Blacklist

A list of entities that are blocked or denied privileges or access.

Source: CNSSI 4009-2015 (NIST SP 800-94)

Breach

Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

Source: ISO/IEC 27040

(adapted)

Common Vulnerabilities and Exposures (CVE)

A nomenclature and dictionary of security-related software flaws.

Source: CNSSI-4009-2015 (NIST SP 800-126 Rev. 2)

Compromise

A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Source: CNSSI-4009-2015

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: CNSSI 4009-2015, NIST SP 800-39

Continuous Monitoring

Maintaining ongoing awareness to support organization risk decisions.

Source: CNSSI 4009-2015 (NIST SP 800-137)

Critical infrastructure

System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Source(s): NIST SP 800-30

Critical infrastructure Sector

A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.

Source: NIPP 2013 Partnering for Critical Infrastructure Security and Resilience

Cryptography

The use of mathematical techniques to provide security services such as confidentiality, data integrity, entity authentication, and data origin authentication.

Source: NIST SP 800-130

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: CNSSI 4009-2015 (NSPD-54/HSPD-23)

Data Loss

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Source: CNSSI 4009-2015 (NIST SP 800-37)

Decipher

Convert enciphered text to plain text by means of a cryptographic system.

Source: CNSSI 4009-2015

Decryption

The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Source: NIST SP 800-133

Denial of Service

The prevention of authorized access to resources or the delating of time-critical operations.

Source: NIST SP 800-33

Digital Forensics

The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Source: NIST SP 800-86

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1) origin authentication, 2) data integrity, and 3) signer non-repudiation.

Source: FIPS 140-2

Disruption

An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Source: NIST SP 800-34 Rev. 1

Encrypt

Cryptographically transform data to produce cipher text.

Source: CNSSI 4009-2015

Encryption

The process of changing plain text into ciphertext for the purpose of security or privacy.

Source: NIST SP 800-21 Second Edition (NIST SP 800-57)

Endpoint Protection Platform

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.).

Source: NIST SP 800-128

Event

Any observable occurrence in a network or system.

Source: CNSSI 4009-2015 (NIST SP 800-61 Rev. 2)

Exfiltration

The unauthorized transfer of information from an information system.

Source: CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)

Exploit

A technique to breach the security of a network or information system in violation of security policy.

Source: ISO/IEC 27039 (adapted)

Firewall

The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Source: NIST SP 800-130

Hack

Unauthorized attempt or access to an information system.

Source: CNSSI 4009-2015 (Adapted from "Hacker")

Hacker

Unauthorized user who attempts to or gains access to an information system.

Source: CNSSI 4009-2015

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Source: NIST SP 800-152

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: FIPS 200

Incident Handling

The mitigation of violations of security policies and recommended practices.

CNSSI 4009-2015, NIST SP 800-61 Rev. 2

Incident Response Plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

Source: CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)

Indicator

A sign that an incident may have occurred or may be currently occurring.

Source: NIST SP 800-61 Rev. 2

Information Operations (I/O)

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO.

Source: CNSSI 4009-2015

Information security policy

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Source: NIST SP 800-128 (CNSSI 4009)

Information system resilience

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Source: CNSSI 4009-2015 (NIST SP 800-39)

Information technology

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources.

Source: NIST SP 800-64 Rev. 2

Insider threat

An entity with authorized access (i.e., within the security) that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-53 Rev. 4 (CNSSI 4009)

Interoperability

A measure of the ability of one set of entities to physically connect to and logically communicate with another set of entities.

Source: NIST SP 800-130

Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Source: CNSSI 4009-2015 (IETF RFC 4949 Ver 2)

Intrusion Detection and Prevention

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Source: NIST 800-94

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Source: NIST SP 800-111

Multifactor Authentication

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Source: NIST SP 800-53 Rev. 4

Non-repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Source: NIST SP 800-32

Outside Threat

An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-32

Password

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Source: FIPS 140-2

Patch

An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Source: NIST SP 800-123

Penetration Testing

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Source: NIST SP 800-115

Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Source: SP 800-45 Ver 2

Port

The entry or exit point from a computer for connecting communications or peripheral devices.

Source: NIST SP 800-82 Rev. 2

Port scanning

Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Source: NIST SP 800-82 Rev. 2 (NIST SP 800-61)

Private key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

Source: FIPS 186-4

Probe

A technique that attempts to access a system to learn something about the system.

Source: CNSSI-4009

Public key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.

Source: FIPS 186-4

Quarantine

To store files containing malware in isolation for future disinfection or examination.

Source: NIST SP 800-114

Resilience

The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Source: NIST SP 800-137 (Adapted from NIST SP 800-39)

Risk analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

NIST SP 800-33

Risk assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

NIST SP 800-33

Scanning

Sending packets or requests to another system to gain information to be used in a subsequent attack.

Source: CNSSI 4009-2015

Spear Phishing

A colloquial term that can be used to describe any highly targeted phishing attack.

Source: CNSSI 4009-2015

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system.

Source: CNSSI 4009-2015

Structured Query Language (SQL) injection

An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Source: US-CERT SQL Injection Publication

Supplier

Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers.

Source: NIST SP 800-161 (Adapted from ISO/IEC 15288, NIST SP 800-53 Rev. 4)

Supply Chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Source: CNSSI 4009-2015

System Integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Source: CNSSI 4009-2015 (NIST SP 800-27 Rev. A)

Tabletop Exercise

A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Source: NIST SP 800-84

Target of Attack

An information technology product or system and associated administrator and user guidance documentation that is the subject of an attack.

Source: FIPS 140-2 (Adapted from Target of Evaluation)

Threat

Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Source: CNSSI 4009-2015 (NIST SP 800-31 Rev. 1)

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Source: CNSSI 4009-2015

Unauthorized access

Any access that violates the stated security policy.

Source: CNSSI 4009

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Source: FIPS 200 (Adapted from CNSSI 4009-2015)

Whitelist

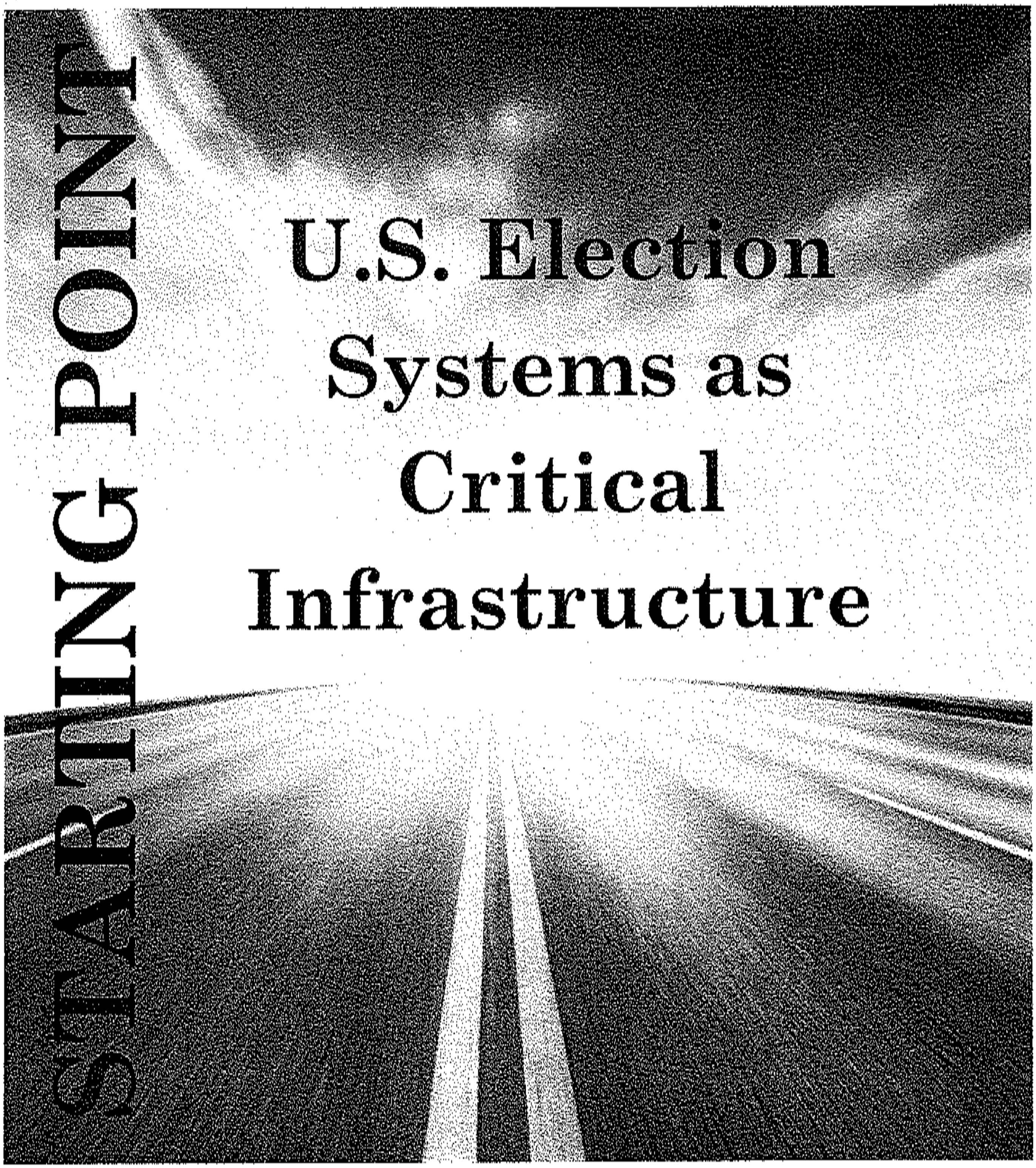
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

Source: NIST SP 800-167

Election Assistance Commission (EAC)

U.S. Election Systems as Critical Infrastructure Addendum I: Glossary of Key Terms and Acronyms

February 2017



STARTING POINT

U.S. Election Systems as Critical Infrastructure

U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

12

Starting Point:

U.S. Election Systems as Critical Infrastructure

On January 6, 2017, Department of Homeland Security (DHS) Secretary Jeh Johnson designated U.S. election systems as part of the nation's critical infrastructure, a decision that was later affirmed by current DHS Secretary John Kelly. Since the designation was announced, state and local election officials across the country have raised questions about the day-to-day impact of the designation and how it will benefit their work to conduct accessible, accurate and secure elections. This document details DHS's critical infrastructure designation and what election administrators can expect moving forward. It also provides a glossary of terms frequently used in conjunction with correspondence and discussions about the critical infrastructure designation.

What is critical infrastructure?

Critical infrastructure is a DHS designation established by the Patriot Act and given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [i] DHS, the department responsible for critical infrastructure, was established by the Homeland Security Act in 2002.

In order to fulfill its responsibilities under the Patriot Act, DHS uses the National Infrastructure Protection Plan (NIPP) as the foundational document, or "rule book," for how to develop sector-specific critical infrastructure plans. The NIPP established a process roadmap by which the nation's critical infrastructure sectors can be identified and created.

In addition to the Patriot Act and NIPP, a third piece of critical infrastructure governing authority comes from Presidential Policy Directive 21 (PPD-21). Released on February 12, 2013, PPD-21 established the Federal Government's "strategic imperatives" in its approach to the nation's critical infrastructure. It established the current critical infrastructure sectors and identified each sector's Sector Specific Agency (SSA), which is the agency charged with structuring and managing the sector.

What other sectors are included in the nation's critical infrastructure?

Critical infrastructure sectors are groupings based on common function and form. There are currently 16 sectors. They are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems. [ii]

One critical infrastructure sector, Government Facilities, has three sub-sectors, Elections, National Monuments and Icons, and Education Facilities. Subsectors are sections of a specific sector that vary from the rest of the sector substantially enough to justify creating a plan just for the subsector.

How are sectors organized?

Once DHS creates a sector, the SSA structures it and helps it self-organize, a requirement of the NIPP. With regard to election systems, this means that members of the election community come together to join and manage the various components that make up this sector. After the critical infrastructure sector is formally established and organized, the SSA is charged with managing it. The SSA is "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." [iii]

While DHS has vast national security knowledge and resources, it acknowledges that it is not an issue-area expert for some of the sectors designated as critical infrastructure. To fill this knowledge gap, DHS will often appoint another federal agency as its Co- Sector Specific Agency (Co-SSA). This is especially common when DHS creates a subsector. Co-SSAs help DHS navigate the nuances of a specific subsector and share SSA responsibilities. For example, the sub-sector Co-SSA for Education Facilities is the Office of Safe and Drug-Free Schools in the Department of Education. A complete list of the sectors, and their respective SSAs and Co-SSAs follows at the end of this document (Addendum II).

DHS has yet to designate a Federal Agency as a Co-SSA for the elections sector. The U.S. Election Assistance Commission (EAC) has publicly called on DHS to select the commission to fill this important role. The request was made in light of the working relationship between DHS and the EAC, crafted during the 2016 presidential election and continued since.

Beyond the SSA and Co-SSA roles, there are other key entities established to support a newly designated critical infrastructure sector, including:

- ✓ **Sector Coordinating Councils (SCCs)**: These are "self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, who interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities." [iv]
- ✓ **Government Coordinating Councils (GCCs)**: These consist of "representatives from across various levels of government (including Federal and State, local, tribal and territorial), as appropriate to the operating landscape of each individual sector, these councils enable interagency, intergovernmental,

and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts." [v]

As part of its designation plan, the SSA will work to establish these councils to support the U.S. election systems designation. For the U.S. election system, these groups will likely include representatives from federal, state, and local government; election system vendors; and other stakeholders impacted by the critical infrastructure designation.

Another key component of operating a critical infrastructure sector is to ensure clear, strong lines of communication between the SSA, Co-SSA, coordinating councils, and stakeholders. This can include creation of the following:

- ✓ **Information Sharing and Analysis Centers (ISACs)**: These are "operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." (Source: Presidential Decision Directive 63, 1998)[vi]
- ✓ **Information Sharing and Analysis Organizations (ISAOs)**: Though similar to ISACs, ISAOs are "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing Critical Infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing Critical Infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to Critical Infrastructure or protected systems; and (c) Voluntarily disseminating Critical Infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b)." [vii]

The distinction between an ISAC and an ISAO is that "[u]nlike ISACs, ISAOs are not directly tied to Critical Infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc." [viii] Essentially, ISAOs allow for more widespread information sharing across sectors and among interested individuals regardless of clearance, knowledge level, or inclusion in a critical infrastructure sector.

What is unique about the protection of critical infrastructure communications?

Information about security and vulnerabilities that is shared under the restrictions of the Critical Infrastructure Information Act is considered Protected Critical Infrastructure Information (PCII). PCII is not subject to the many disclosure regulations, such as those found in the Freedom of Information Act and its state-level counterpart. This protection, allows the critical infrastructure community to discuss vulnerabilities and problems without publically exposing potentially sensitive information.[ix]

For those participating in election sector coordinating councils this protection means that some information communicated between DHS and the coordinating councils can be protected. This limits the potential for sensitive election security information to be made public and protects potentially sensitive material from being misconstrued or used for nefarious purposes. This protection is made possible by an exception to the Federal Advisory Committee Act created by the Critical Infrastructure Partnership Advisory Council.[x]

Are new resources available following a critical infrastructure designation?

A critical infrastructure designation provides for greater access to DHS information and security resources. It also provides a safer and more discreet exchange of information and requests for advice or assistance. While it is important to note that DHS will provide assistance to any domestic entity that requests help and not just critical infrastructure, its assistance to entities within a critical infrastructure sector is prioritized over providing assistance to non-critical infrastructure entities.

DHS resources – including on-going and current information about threats, risk and vulnerability assessments, and security best practices as well as hands-on advice – help infrastructure owners and managers better secure their systems. The department emphasizes the importance of the information assets it has available to critical infrastructure entities and understands that security clearances are a requirement for accessing some of these resources. This is why DHS works with infrastructure owners and managers to secure clearances when necessary.

Use of DHS resources and participation in sector councils is voluntary, and DHS continually states that it cannot force critical infrastructure owners and managers to interact with a sector, its components, or its resources. Entities that choose to leverage these new resources have a direct line to DHS resources via a Cyber Security and Protective Security Advisor. These advisors directly supply security assistance to the country and handle on-going assistance to CI entities.

While some within the election community remain skeptical about the critical infrastructure designation, their outstanding concerns about the designation make the case for why input from key election sector stakeholders is a vital part of setting up the needed infrastructure of councils and committees that can make this designation impactful. DHS is actively seeking participation from election stakeholders and their sector allies, noting that there is an advantage inherent in helping to shape the critical infrastructure mechanisms election officials will use to gain resources and communicate with DHS. The department has relied on the EAC to provide the forum for much of this outreach, and the commission recommends that election officials and others in the election community take steps to becoming involved in this process either directly or through the EAC.

What role will the EAC play as DHS stands up the critical infrastructure designation?

The EAC has requested DHS name the commission as Co-SAA. This designation is important to ensure that state and local election officials and administrators have an informed federal advocate working directly with DHS as the department determines what resources and services are needed to protect U.S. election systems and how these resources will be distributed. The EAC has held and will continue to hold, hearings and meetings to give DHS a platform to discuss the designation and its potential benefits, as well as answer questions from stakeholders. The EAC prides itself on serving as a trusted intermediary between state and local election officials and federal government leaders, as well as a provider of resources needed to navigate this new space. Serving as the official Co-SSA for implementing the critical infrastructure designation would tap into this strength and provide election officials with assurance that their interests and concerns will shape the contours of DHS's plan moving forward.

Addendum I: Glossary of Key Terms and Acronyms

Critical Infrastructure Glossary

Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source:§1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and State, local, tribal and territorial governments. (Source: CIPAC Charter) These meetings are exempt from the Federal Advisory Committee Act (FACA) requirements that they be open to the public and provide meeting materials to the public.
Critical Infrastructure Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and State, local, tribal and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998) ISACs are not operated, controlled, or managed by DHS.

Information Sharing and Analysis Organization (ISAO)	"Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability there of; communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)." (Source: Homeland Security Act of 2002)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
National Annual Report	Each SSA is required to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. (National Infrastructure Protection Plan: The National CI/KR Protection Annual Report)
National Infrastructure Coordinating Center (NICC)	The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	The National Infrastructure Protection Plan 2013, involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry, provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes, provides an updated approach to critical infrastructure security and resilience, and involves a greater focus on integration of cyber and physical security efforts. (DHS, NIPP Fact Sheet)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	[The DHS division] that leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance). NPPD contains the Federal Protective Service, the Office of Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.

Presidential Policy Directive 21 (PPD-21)	[Presidential Directive that] Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and State, local, tribal and territorial entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Presidential Policy Directive 8 (PPD-8)	[Presidential Directive that] facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Protected Critical Infrastructure Information (PCII)	PCII is [information and communications] protected from disclosure. All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. Critical infrastructure information voluntarily shared with the government and validated as PCII by the Department of Homeland Security is protected from, the Freedom of Information Act (FOIA), State, local, tribal, and territorial disclosure laws, use in regulatory actions and use in civil litigation. PCII can only be accessed in accordance with strict safeguarding and handling requirements, and only trained and certified federal, state, and local government employees or contractors may access PCII.(Source: CII Act of 2002, 6 U.S.C. § 131, and www.dhs.gov/pcii-program)
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts who work for DHS and are responsible for ensuring all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operator. There are three types: (1) Regional Directors, supervisory PSAs, PSAs, and geospatial analysts. s. (Source: DHS.gov/protective-security-advisors)
Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)

Addendum II: Critical Infrastructure Sectors and their SSAs and Co-SSAs

Sector/ Subsector	SSA	Co-SSA
Chemical	Department of Homeland Security (DHS)	
Commercial Facilities	Department of Homeland Security (DHS)	
Communications	Department of Homeland Security (DHS)	
Critical Manufacturing	Department of Homeland Security (DHS)	
Dams	Department of Homeland Security (DHS)	
Defense Industrial Base	Department of Defense (DOD)	
Emergency Services	Department of Homeland Security (DHS)	
Energy	Department of Energy (DOE)	
Financial Services	Department of the Treasury	
Food and Agriculture	Department of Agriculture (USDA)	Department of Health and Human Services (HHS)
Government Facilities	Department of Homeland Security (DHS)	General Services Administration (GSA)
Elections (subsector)	Department of Homeland Security (DHS)	
Education Facilities (subsector)	Department of Homeland Security (DHS)	Department of Education
National Monuments (subsector)	Department of Homeland Security (DHS)	Department of the Interior (DOI)
Healthcare and Public Health	Department of Health and Human Services (HHS)	
Information Technology	Department of Homeland Security (DHS)	
Nuclear Reactors, Materials, and Waste	Department of Homeland Security (DHS)	
Transportation Systems	Department of Homeland Security (DHS)	Department of Transportation (DOT)
Water and Wastewater Systems	Environmental Protection Agency (EPA)	

[i] Patriot Act, (Sec. 1016(e))

[ii] https://www.dhs.gov/Critical-Infrastructure-sectors, accessed May 2, 2017.

[iii] Ibid.

[iv] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, p. 12.

[v] *NIPP 2013*, p. 31.

[vi] Presidential Decision Directive 63, 1998.

[vii] Source: *Homeland Security Act of 2002, 6 U.S.C. § 131.*

viii Department of Homeland Security, Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs), https://www.dhs.gov/isao-faq, accessed May 3, 2017.

[ix] Department of Homeland Security, *NIPP 2013*, p. 12.

[x] Department of Homeland Security, *United States Department of Homeland Security Charter of the Critical Infrastructure Partnership Advisory Council*, https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf, accessed June 5, 2017

Harvard Kennedy School Belfer Center
Campaign Cybersecurity Playbook

November 2017

HARVARD Kennedy School
BELFER CENTER

REPORT - *Belfer Center for Science and International Affairs, Harvard Kennedy School*

Cybersecurity Campaign Playbook

November 2017

Welcome

People join campaigns for different reasons: electing a leader they believe in, advancing an agenda, cleaning up government, or experiencing the rush and adrenaline of campaign life. These are some of the reasons we got involved in politics. We certainly didn't sign up because we wanted to become cyber experts and we're guessing you didn't either.

We come from different political parties and don't agree on much when it comes to public policy, but one thing uniting us is the belief that American voters should decide our elections and no one else. Our increasingly digital way of living and working offers new ways for adversaries to influence our campaigns and elections. While you don't need to be a cyber expert to run a successful campaign, you do have a responsibility to protect your candidate and organization from adversaries in the digital space. That's why Defending Digital Democracy, a project of Harvard Kennedy School's Belfer Center for Science and International Affairs, created this **Cybersecurity Campaign Playbook [PDF]**.

The information assembled here is for any campaign in any party. It was designed to give you simple, actionable information that will make your campaign's information more secure from adversaries trying to attack your or-ganization—and our democracy. Most of all,

Table of Contents

we hope this resource allows you to spend more time on what you signed up for—campaigning.

VI. Authors & Contributors

Good luck.

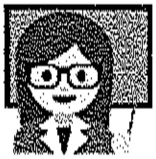
Robby Mook
Hillary Clinton 2016 Campaign Manager

Matt Rhoades
Mitt Romney 2012 Campaign Manager

P.S. Do you see a way to make the Playbook better? Are there new technologies or vulnerabilities we should address? We want your feedback. Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #CyberPlaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Top Five Checklist

1. Set the Tone:



Take cybersecurity seriously. Take responsibility for reducing risk, train your staff, and set the example. Human error is the number one cause of breaches.

2. Use the cloud:

A big, commercial cloud service will be much more secure than anything you can set up. Use a cloud-based office suite like GSuite or Microsoft365 that will provide all your basic office functions and a safe place to store information.

3. Use two-factor authentication:

Require 2FA for all important accounts, including your office suite, any other email or storage services, and your social media accounts. Use a mobile app or physical key for your second factor, not text messaging.

4. Create strong, long passwords:

For your passwords, create SOMETHINGREALLYLONGLIKETHISSTRING, not something really short like Th1$. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with L0t$ of $ymB01$. A password manager can help, too.

5. Plan and prepare:

Have a plan in case your security is compromised. Know whom to call for technical help, understand your legal obligations, and be ready to communicate internally and externally as rapidly as possible.

The Playbook Approach

This Cybersecurity Campaign Playbook was written by a bipartisan team of experts in cybersecurity, politics, and law to provide simple, actionable ways of countering the growing cyber threat.

Cyber adversaries don't discriminate. Campaigns at all levels – not just presidential campaigns – have been hacked. You should assume you are a target. While the recommendations in this playbook apply universally, it is primarily intended for campaigns that don't have the resources to hire professional cybersecurity staff. We offer basic building blocks to a cybersecurity risk mitigation strategy that people without technical training can implement (although we include some things which will require the help of an IT professional).

These are baseline recommendations, not a comprehensive reference to achieve the highest level of security possible. We encourage all campaigns to enlist professional input from credentialed IT and cybersecurity professionals whenever possible.

Introduction

Candidates and campaigns face a daunting array of challenges. There are events to organize, volunteers to recruit, funds to raise, and the relentless demands of the modern media cycle. Every staffer must anticipate unfortunate surprises like gaffes or a last-minute attack ad. Cyber attacks now belong on this list as well.

As campaigns have become increasingly digital, adversaries have found new opportunities to meddle, disrupt, and steal. In 2008, Chinese hackers infiltrated the Obama and McCain campaigns, and stole large quantities of information from both. In 2012, the Obama and Romney campaigns each faced hacking attempts against their networks and websites. In 2016, cyber operatives believed to be sponsored by Russia stole and leaked tens of thousands of emails and documents from Democratic campaign staff.

The consequences of a cyber breach can be substantial. News of a breach itself, compounded by a slow-drip release of stolen information, can derail a candidate's message for months. Attackers overloading a website can lead to lost donations at key moments. The theft of personal donor data can generate significant legal liabilities and make donors reluctant to contribute to a campaign. Destructive attacks aimed at staff computers or critical campaign servers can slow down campaign operations for days or even weeks. Cleaning up the resulting mess will divert precious resources in the heat of a close race, whether it's for president or city council.

For the foreseeable future, cyber threats will remain a real part of our campaign process. As democracy's front line, campaign staff must recognize the risk of an attack, develop a strategy to reduce that risk as much as possible, and implement response strategies for that moment when the worst happens. While no campaign can achieve perfect security, taking a few simple steps can make it much harder for malicious actors to do harm. Ironically, the most sophisticated state actors often choose the least sophisticated methods of attack, preying on people and organizations who neglect basic security protocols. That is our primary reason for creating this Cybersecurity Campaign Playbook.

In today's campaigns, cybersecurity is everyone's responsibility. Human error has consistently been the root cause of publicized cyber attacks, and it's up to the candidate and campaign leaders to weave security awareness into the culture of the organization. The decisions humans make are just as important as the software they use. Going forward, the best campaigns will have clear standards for hard work, staying on message, being loyal to the team—and following good security protocol.

Before we get into our recommendations, let's quickly frame the problem:

- the **environment** in which your campaign is operating;
- the **threats** your campaign will likely face; and,
- the **importance** of cyber risk management.

The Threats Campaigns Face

Unfortunately for campaigns and our country, foreign adversaries may think that harming or helping a particular candidate advances their national interest, whether that means creating chaos and confusion among American voters, or punishing an official who has spoken out against them. This may sound like thriller fiction, but the reality is that a sophisticated foreign intelligence service, cybercriminal or hacktivist with a grudge against a candidate, could decide that you or someone on your campaign is a target.

These are the sorts of threats managers and staffers have to realize are possible.

WHO'S HACKING?

Campaigns face information and cybersecurity threats from a wide array of actors. Lone "black hat" hackers and cybercriminals have tried compromising campaigns for reasons of personal gain, notoriety, or the simple desire to see if they could. Nation-states pose the most dedicated and persistent threat. Russian espionage groups known as "Fancy Bear" (APT 28) and "Cozy Bear" (APT 29) were implicated in the 2016 campaign hacks. The Chinese have focused much more on information gathering. They are believed to have been active in the 2008 and 2012 presidential campaigns, but there is no evidence they released any stolen materials. The North Koreans infamously retaliated against Sony Pictures Entertainment for producing the film, The Interview, by stealing and releasing company emails and wiping their systems. Heightening tensions with the United States could prompt more attacks in the future.

Managing Cyber Risk

Risk is best understood in two parts. First, there are **vulnerabilities**: weaknesses in your campaign that make information susceptible to theft, alteration, or destruction. Vulnerabilities can originate in hardware, software, processes, and in the vigilance of your staff. Second are the actual **threats**: the nation states, hacktivists, and other nonstate groups with the capability to exploit those vulnerabilities. Risk results where threat and vulnerability meet.

There's nothing you or your campaign can do to prevent threats themselves – they are the result of larger geopolitical, economic, and social forces. What you can do is substantially reduce the likelihood that your adversaries will succeed by reducing how vulnerable you are. Reducing vulnerability reduces risk – it's up to you to decide which ones are most essential to reduce. For example, you may decide that the most damaging thing a hacker could do is to steal your candidate's self research report, so you will devote extra resources for secure cloud-based storage, require long passwords and restrict access to a small number of people. You may decide to make other documents on the campaign more widely available and less secure, since more people need them to do their job and they wouldn't cause much damage if they were leaked.

There are technical aspects to risk mitigation and we have many technical recommendations in this playbook, but what matters most is your holistic approach. As a campaign leader, the most important thing you can do is make fundamental choices, such as who has access to information, what information is kept or discarded, how much time you devote to training, and your own behavior as a role model. As a campaign professional, risk management is your responsibility –

both technical and human. It's up to you to decided what data and systems are most valuable and what resources you commit to protect it.

Securing Your Campaign

Our security recommendations are organized according to three principles:

1. Prepare: The success of nearly every one of the Playbook's recommendations depends on the campaign manager creating a culture of security vigilance that minimizes weak links. That means establishing clear ground rules that are enforced from the top down and are embraced from the bottom up.

2. Protect: Protection is critical. When you discover you have a security problem, it is already too late. Building the strongest defenses that time and money allow is key to reducing risk. Internet and data security works best in layers: there is no single, bulletproof technology or product. A few basic measures used in combination can make a campaign's digital architecture more difficult to breach and more resilient if compromised.

3. Persist: Campaigns now face adversaries with ever-increasing levels of resources and expertise; even the most vigilant culture and the toughest infrastructure may not prevent a security breach. Campaigns need to develop a plan ahead of time to deal with a breach if one occurs.

Some campaigns have more time and money for cybersecurity than others. That's why our recommendations offer two tiers of protection: "**good**" and "**enhanced.**" The "good" tier represents everything a campaign **must** do to have a **minimum** level of security. Using the "good" recommendations in a piecemeal fashion will leave you vulnerable. You should always aspire to do more as time, money, and people allow, which is why we recommend using the "enhanced" level whenever possible. If you have the resources to get reputable, trained IT support, it's money well spent. Threats are constantly evolving and professional IT services will help get you beyond what this playbook provides and keep you abreast of the latest threats and solutions.

Management

Campaign managers need to take responsibility for their cybersecurity strategy, but most will delegate development and supervision to a deputy or operations director. It's important that cybersecurity is tightly integrated into HR and IT work, since correctly onboarding staff, provisioning hardware, and controlling permissions will be critical to your strategy. Many small campaigns will rely on volunteer support for IT and cybersecurity. You can use this playbook to guide your discussion with your volunteer support. The key is to carefully vet the volunteers who support you and carefully control access, so that volunteer support doesn't create new vulnerabilities. You should make sure a campaign staffer is supervising IT work and controlling permission to access different systems.

When To Start

Whatever support model you have, *cybersecurity should start on Day One*. What follows is a "top five checklist" of measures that are absolutely vital. Make sure these are in place at the very beginning, even if there are just one or two staff, then complete the other "good" recommendations as soon as possible.

Cost

A lot of what we recommend here is free or very low cost. In fact, everything on our top five list is free, except getting a cloud-based platform, which will only cost a few dollars per month per employee. High target campaigns will need to budget enough resources for hardware and software to execute a responsible strategy, but this should still be a very small percentage of a multi-million dollar statewide campaign budget. Smaller campaigns will be able to execute the recommendations here for a few hundred to a few thousand dollars depending on how many staff or volunteers work on the campaign.

Any references to vendors and products are intended to help provide examples of common solutions, but do not constitute endorsements. If challenges arise when implementing products or services, we encourage you to reach out directly to the vendors, who can usually provide user-level technical assistance. When it comes to product and service selection, we encourage every campaign to consult with a cybersecurity expert or conduct independent research to find the best product for their needs.

The Vulnerable Campaign Environment

Today's campaigns are uniquely soft targets. They're inherently temporary and transient. They don't have the time or money to develop long-term, well-tested security strategies. Large numbers of new staff can be on-boarded quickly without much time for training. They may bring their own hardware from home – and the malware lurking on it! Things move fast, the stakes are often high, and people feel like they don't have the time to care about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, campaigns rely more and more on proprietary information about voters, donors, and public opinion. They also store sensitive documents like opposition research, vulnerability studies, personnel vetting documents, first-draft policy papers, and emails. The risks of a potential attack are increasing and so are the consequences.

THE DANGER OF AN ATTACK

Picture this: It's a month before Election Day, and the race is tight. You arrive at headquarters early, fire up the coffee maker, get to your desk, and log into your computer. A black screen pops up, then a gruesome cartoon of your candidate, followed by a message. Your hard drives have been wiped clean. Every digital bit of information you've gathered—memos, targeting lists, balance sheets—is gone. Getting it back, you read, will cost a cool million in Bitcoin and the renunciation of a major policy position.

An unidentified group hacked into your computer months ago, and has been quietly stealing emails, strategy memos, donors' addresses, and staffers' Social Security numbers. The group has spent weeks combing through the bounty in search of dirty laundry and created an easy-to-use website dedicated solely to distributing the highlights. Prominently featured is a lengthy "self research" book on your candidate. For now, the campaign's website is down, its social media accounts have been suspended for pushing out lewd images, and there's not a working computer in sight.

Steps to Securing Your Campaign

STEP 1: The Human Element

Cybersecurity is fundamentally a human problem, not a technical one. The best technical solutions in the world will have no effect if they are not implemented properly, or if they are not continuously updated as technology evolves. Successful cybersecurity practices depend upon creating a culture of security.

1. Establish a strong information security culture that emphasizes security as a standard for a winning campaign. Just as campaign staffers are instructed not to take an illegal donation, employees should know to avoid clicking on links or opening attachments in emails from unknown senders.
   - Onboarding: Provide basic **information security training** when you onboard new staff. You can distribute the Staff Handout at your training.
   - Trainings: Make security part of all your ongoing **staff trainings**, such as senior staff retreats or GOTV trainings. Provide **additional training** for those in sensitive roles, such as the candidate, press staff, senior staff, and anyone with system administrator privileges on your network. Managers should require that the most important people in the campaign—including the candidate—have their security settings checked by whoever runs IT (that may be the manager herself). Don't be timid or half-hearted about security for the candidate and other VIPs!
   - Set the example: Senior campaign staff and the candidate must take a **visible leadership role**, advocating for cybersecurity during trainings. Senior staff should provide **periodic reinforcement** of cybersecurity's importance to junior staff in meetings and on calls. Don't just have technical experts conduct trainings. The campaign manager or operations director can be a more powerful messenger precisely because they're seen as less "technical."

2. Conduct a thorough **vetting** of staff, volunteers, and interns—anyone requesting access to campaign information—to avoid giving credentials to someone who wants to steal or sabotage your systems. Establish a definition for **sensitive information** and rules for its use. For example, you could choose to classify all polls, research materials, strategy memos, and related emails as "sensitive." Prohibit the transfer of sensitive information on communication channels that aren't managed and secured by the campaign. You can require that it be transferred only through encrypted messaging (see Step 2).

3. **Confirm that consultants and vendors with access to sensitive information have secure email and storage** (see Step 2). When in doubt, require vendors and consultants to use an account on your cloud-based office suite (See Step 2).

4. **Control access** to important online services, such as the official campaign social media accounts, to prevent use by unauthorized individuals. Make sure that those who leave the campaign can no longer access campaign-related accounts. You can do this easily by using a social media account management tool that acts as a gateway to all your accounts. If someone leaves the campaign, you should immediately disable their account.

5. **Educate staffers about the phishing threat**. Make sure they know how to spot and avoid suspicious links and emphasize the importance of identifying and reporting potential phishing

attacks. As part of the campaign's strong security culture, senior staff should recognize and praise anyone who reports suspicious behavior on their system or admits to clicking a potentially malicious link.

Handouts

For Staff Members

For Family Members

1. Software products such as Phishme and KnowBe4 can **train your staff by sending them fake phishing emails**. This is a safe, quick, and effective way to learn who is at risk of clicking a link, so you can give them counseling and extra training. Many of these products also filter some phishing attempts out of your email.
2. If you have the resources, **hire a dedicated IT professional** to manage your campaign's systems and an IT security expert to help protect, maintain, and monitor your campaign's digital infrastructure. He or she can provide regular security training and testing of your people and systems, while customizing security solutions.
3. **Contract with a cybersecurity firm** to provide security solutions, review your defenses, and/or monitor your systems for a breach. Know which firm you want to contact if you are breached and need urgent incident response support. This is an alternative to hiring a full-time IT security expert. Do your research and go with a highly reputable, U.S.-based firm—not all cybersecurity firms provide the same level of service.

WORKING WITH SECURITY PROFESSIONALS

If you decide to work with a security professional, how will you evaluate the right person or firm? Whether it's through personal recommendations or positive public reviews, it's important that you avoid costly yet ineffective support. When interviewing potential security professionals, ask about how they've responded to past security incidents and how they've enabled others to work more securely. Your respective national party committee or trusted campaign professionals may be able to recommend options to choose from. Bear in mind that culture affects security and that even the best recommendations may fail to achieve results if they are not followed (i.e., just hiring a firm won't solve your problems).

STEP 2: Communication

Not all methods of communication are equally secure, so use the most secure method possible. Campaign leadership should set a standard that encourages in-person conversations whenever possible, and discourages needless or superfluous emails. Whether it is phone calls, texting, or emailing, different products and services offer different levels of protection, so do your research before you choose which systems your campaign is going to use.

WHAT IS THE CLOUD?

"Cloud services" provide management and access to information stored remotely on the Internet. They run on off-site servers managed by third-party companies; this includes many common services you may already use, such as Gmail or Dropbox. It's good to store information in the cloud instead of on your personal computer because big cloud providers have the money and expertise to make their server farms more secure than your laptop's hard drive, or an office server. **It's like the difference between leaving cash under your mattress and storing it in a bank's security vault.** Using cloud services offers an additional backstop against data loss if an individual device is lost or compromised. Cloud storage is a feature included in comprehensive office security services such as GSuite and Microsoft365. Other services include Dropbox or Box.

1. Use a **cloud-based office suite** that provides secure email communication, document creation, chat, and file sharing, such as GSuite or Microsoft365. For example, GSuite includes Google Drive for file sharing, Gmail for email hosting, Google Hangouts for chat, and Google Docs for word processing, spreadsheets, and presentations. Microsoft365 offers OneDrive/SharePoint for file sharing, Outlook/Exchange for email, Microsoft Teams for chat, and Microsoft Office for word processing, spreadsheets, and presentations. Cloud-based systems managed by major firms will be better protected than any servers you could set up in your campaign. There are free versions of both products, but the paid versions give you many more administrative capabilities. Google also offers a service called *Protect Your Election* that will provide extra protection against phishing for their free email service.They also offer a free service to protect your website against disabling attacks.

2. Use the most secure systems possible for communication.
   - Use **encrypted messaging** services such as Signal, Wickr, especially for messages, document sharing and phone calls. Many campaigns require that sensitive information only be transmitted by encrypted messaging, although you can use it for all communication if you want (this is especially smart for high-risk individuals like the candidate). Signal and Wickr allow you to auto-delete messages, which reduces risk.
   - Switch off archiving for messaging services, such as Google Chat and Slack, so that old chats can't be stolen later. This requires going into "settings" and adjusting "retention policy" timelines. Some services require you to do this for every single chat conversation. We recommend retaining chat messages for one week or less.

3. Defend your email
   - **Turn on Auto-delete** in your email application for old emails to reduce the number of emails that could potentially be stolen. This usually requires going in and changing "retention policy" to shorter time periods in "settings." To ensure emails do not just sit in a "deleted items" folder, adjust settings to auto purge "deleted items" folder after a certain time period. We recommend retaining emails for one month or less.

4. Secure personal accounts
   - Campaign business should never go on personal accounts. However, adversaries will target personal accounts for hacking, so have your staff use strong passwords and two-factor for their personal accounts as well (this is included in our Staff Handout).

WHAT IS ENCRYPTION?

Encryption is a way of encoding information when it travels between users, or when it's stored, so it can't be read by anyone but the intended recipient. Think of it this way: a user "scrambles" the data when she sends it and only the intended recipient has the key to unscramble it. Using encryption is smart, especially for sensitive information, because even if an adversary steals the data, it's unlikely they'll be able to read it. Most apps that use encryption, like Signal or Wickr, make the process seamless. Laptops or cloud storage systems use encryption as well.

STEP 3: Account Access and Management

One of the most challenging aspects of security is keeping unauthorized people out. This means preventing adversaries from gaining access to your data and preventing people within your campaign from having access to information they do not need. While some of the recommendations below may seem cumbersome, hackers depend on those who value convenience over security.

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-factor authentication is a second layer of security that requires a user to provide an extra credential beyond her or his password. The second factor is critical because, if your password is stolen, an adversary still can't log into your account. Your password is something you know and your second factor is something you have, like a code that's generated by an app, a physical key, or even something biometric, like a fingerprint.

1. Require **two-factor authentication** (2FA) on all systems and applications. **Avoid texting (SMS)** for two-factor authentication, because attackers can easily clone a phone number and get access to texts. There are several 2FA apps that work just as well as texting, such as Google Authenticator, Microsoft Authenticator, and Duo Mobile. You can also use a physical FIDO

("fast identity online") key that is inserted into your USB drive such as Yubikey or Feitian. The website "TwoFactorAuth.org" is a helpful guide to services that do and do not offer 2FA.

2. Passwords.
   - **Require strong passwords.** As we noted earlier, "make passwords that are long and strong." Current computing capabilities can crack a seven-character password in milliseconds. A 20-, or even 30-character password will take much longer for a hacker to crack. Choose a string of words that you can easily remember.
   - Use a different password for different accounts so a hacker can't break into multiple accounts if a single password is stolen.
   - If someone reaches out requesting a password or password reset, require the request to be made in person or over a video chat to ensure it is the actual campaign staff member or volunteer. Only share passwords in person or over short-lived encrypted messages. Never share passwords over email or store/distribute using a helpdesk system.
3. **Use password managers** such as LastPass, 1Password, or Dashlane to help you manage a lot of long, strong passwords easily. But ensure that your management system has a long, strong password and two-factor authentication. We don't currently recommend password managers built into browsers, which are often less secure than these standalone managers.
4. Create **separate accounts for administrators and users**, and severely restrict access to administrator accounts. Administrators should also have two separate campaign accounts—one used only for their admin duties and one that is their standard user account for all other campaign business. This will reduce the likelihood that an adversary will be able to compromise an administrator account, which would provide access to the entire network.
5. Conduct **periodic reviews** of who has access to different devices and networks. Immediately block access of people who leave the campaign. Immediately change passwords if suspicious activity is observed.

PASSWORD MANAGERS

Password managers are a way to store, retrieve, and generate passwords. Some even have the ability to auto-populate the password line on login pages. The password manager requires a password of its own to login, which becomes the one password you do have to remember. The risk, of course, is that if someone breaks into your password manager (it has happened), that person will have all of your passwords. But this risk is almost always far outweighed by the benefit of strong, unique passwords across all of your accounts. For campaigns, password managers sometimes make sense for accounts that have multiple users, because the administrator can safely share access to them.

1. Create **user profiles** for different types of campaign staff that automatically grant the necessary level of access. Different types of employees—interns, field staff, campaign leadership—require access to different resources. Having predetermined profiles makes it easier to ensure that people are getting access only to what they need.

WHAT ARE ADMINISTRATORS?

In "IT speak," an "administrator" or "admin" has the ability to give people access or control to systems or information. For example, as the "admin" for an email system, you can create accounts, change passwords, and set requirements like password length and two-factor authentication for all accounts. In an office suite like GSuite or Microsoft 365, you can also create groups, such as the "Field Team" or "Comms Team." An admin's job is really important. If they do things right, information will be available only to people who need it, which is essential for security. This means that deciding who gets admin privileges is also a critical decision. Only a few, highly trusted people should be able to grant others access to information. If a staffer with "admin" privileges leaves the campaign, make sure to take away their privileges immediately!

STEP 4: Incident Response Planning

It's just as important to plan for responding to an attack as it is to develop a security strategy to prevent one. How you respond often has more to do with the ultimate outcome of an incident than what was compromised. You should budget some time at strategic retreats or longer senior staff meetings to discuss what will happen if something does go wrong. Here's a checklist of the steps you should take

LEGAL

✔ **Identify outside counsel** you will retain in the event of a cyber incident, and discuss the response process with them at the outset of the campaign. In most cases, this will be the same person who represents your campaign on other matters, but ideally you would have someone who specializes in incident response on call, either pro bono or for a $0 retainer.

✔ Ask your lawyer to explain **your legal obligations** if data is stolen and what compliance measures you will need to have in place.

✔ Understand **your vendors' legal obligations** to notify you or others if they are hacked. Wherever possible, include strict notification requirements in your vendor contracts, since third parties are a frequent source of breaches.

✔ If you believe you've been breached, a best practice is for **your lawyer to oversee your response** under attorney-client privilege.

✔ Talk to your lawyer about the best way to **work with law enforcement if a breach occurs**. Every campaign will approach this differently.

TECHNICAL:

✔ Determine ahead of time **whom you will call for technical assistance** if you think you've been hacked. Your state caucus or national party committee can usually provide referrals.

✔ Choose **someone on the campaign who will interface with technical experts** in the event of a breach. This is ideally the same person who is already coordinating IT for the campaign. Managing an incident response can be overwhelming, so you want someone focused on the technical aspects who knows what they are doing. That way you can focus on communicating with stakeholders and the press.

OPERATIONS:

✔ Decide in advance who will be on your **Incident Response Team** (IRT) and who will participate in incident response meetings. It's important to include someone from your IT, legal, operations, and communications teams. If you're a small campaign and don't have full-time communications, IT, or operations support, plan to include any key staff who oversee campaign operations.

✔ Determine the **chain of command for decision-making** in the event of a breach, especially regarding communications. In many cases, this will be the campaign manager, but some managers may choose to delegate responsibility to someone else.

✔ Identify what **app or technology you will use to communicate** if you think your email has been breached (Signal and Wickr are two common options). Communication during a breach is essential, but you don't want your adversaries to know what you're saying—or even that you are responding to their actions.

COMMUNICATIONS:

✔ **Conduct scenario planning.** For many campaigns, this can be part of an existing strategy retreat. For bigger campaigns at higher risk, it may be necessary to have a dedicated meeting. Your scenario planning should include:

✔ **Identifying key internal and external stakeholders**, like your staff, volunteers, donors, and supporters. Know whom you need to contact if an incident occurs and rank them in order of priority. Develop a contact list and designate who will reach out to them.

✔ **Brainstorm the most damaging scenarios** and consider how your stakeholders and messaging may change for each one. Different scenarios could include:

- Rumors that your campaign has been hacked;
- Credit card and contact information for your donors is stolen;
- Ransomware and an extortion attempt are lodged against your campaign;
- Your systems are wiped and shut down;
- Someone's emails are stolen;

- Your adversary steals your administrator's credentials and every file on your campaign drive.

✔ **Be careful what you say in the present about cybersecurity policy** or cyber incidents. Some victims of cyber crimes have previously made grandiose pronouncements about their own security measures, or have criticized others who have been attacked. The press will hold you accountable for what you said in the past if you fall victim.

✔ Similarly, **avoid providing details about the scope of the event in the early phases** of the incident (and if you can avoid discussing the scope altogether, even better). Details available at the outset will change as you investigate. A common mistake is to say something that later turns out not to be true (e.g., "they didn't steal very much," or "no personal information was taken"). Saying only what you know for sure is the safest course. Statements should focus on the actions you are taking to make the situation right for the affected stakeholders.

✔ **Develop some boilerplate language** in advance, so that you can draft statements or talking points quickly if an incident occurs. At a minimum, create a simple Q & A document that you can rapidly revise if you actually need to use it. Creating a Q & A document in advance will help you to think as much about what you won't say as what you will say. For example, the first question will often be, "What happened?" However, you may not be able to answer that for days or weeks. The fact that you don't know what kind of breach will take place can actually help you write better boilerplate answers in advance. Questions to include in your Q & A document are [call out box]:

- What happened?
- How did it happen?
- Who did it?
- What was stolen or damaged?
- Was anyone's personal information stolen? What are you doing to protect them?
- How did the hackers do it?
- Are the hackers out of your system?
- How long were they in your system?
- What security measures did you have in place? Why weren't they effective?
- Shouldn't you have known this would happen? Why weren't your systems better secured?
- Are you working with law enforcement? Has law enforcement contacted you?
- In a ransomware breach, you'll be asked: Did you pay the ransom and why or why not?

✔ **Stay in touch with your key stakeholders** and keep them as informed as you can. You probably won't be able to say much, but contacting them regularly with what you do know, having a clear statement about your intentions, and providing details about what you are doing to manage the situation are key. Avoid setting an expectation of too frequent updates, because often you won't have new information and your stakeholders will become frustrated if you continue to return to them without new information. Only speak proactively to the media if you have new information to provide.

STEP 5: Devices

Every physical device in your campaign—from a cell phone, tablet, or laptop to a router, printer, or camera—represents a potential attack path into your network. A good cybersecurity plan will attempt to control access to, into, and on all devices. You can control access to devices by making sure they are always properly handled and accounted for. You control access into devices via two-factor authentication and strong passwords. You control the content on devices via encryption and the policies guiding how you store data (i.e., storing information in the cloud instead of on machines).

1. Always use the most **updated operating system** (OS) available, since system updates regularly include patches for the latest vulnerabilities. If possible, set device settings to **auto-install** these updates. Make it someone's job to check on a regular basis that everyone is current.
2. Use an automatic **cloud-based backup service** to mitigate the impact of data loss if a device is lost or stolen. Examples include Backblaze and CrashPlan.
3. Access to the device
    - From the start, campaign leadership should **create an environment** in which people take physical security of their devices seriously—losing a device could give an adversary access to critical information that can be used to hurt the campaign.
    - Although many campaigns cannot afford to buy new devices, it's always best to **purchase new equipment (especially computers and phones)** if you can. At a minimum, you should provide new devices for personnel who work with sensitive data.

- If staff are using their own computers and phones, **establish a "Bring Your Own Device" (BYOD) policy** that implements strong security practices (see endpoint protection below).
- Campaign members should **NOT use personal email accounts or devices that have not been secured per the BYOD policy** for campaign business, including email and social media. Any important information that resides outside devices or systems controlled by the campaign is vulnerable to attack. Leadership should constantly reinforce that campaign data needs to stay off personal email and unsecured computers.
- Report lost devices immediately. Require default settings that allow for **remote wiping** on all devices.
- Win or lose, have a plan in place for **what happens to all data, accounts, and devices** when the campaign ends. The immediate aftermath of a campaign is an especially vulnerable period.

4. Access into devices.
   - **Change default passwords and settings** on all devices. Many devices come from the factory with a default password that is really easy to guess. Also, disable the guest account if a device comes with one.
   - Implement **auto-lock** for phones and computers after two minutes and require a **password or fingerprint ID** to unlock.
   - Defender. There are special endpoint security apps for phones and tablets. Lookout is an example.

5. Content on devices.
   - Require **encryption** on all devices (computers and phones) to ensure that the loss of a device does not mean the compromise of its content. Examples include FileVault for Mac and BitLocker for Windows. Some devices like the iPhone do this by default, but not all do.
   - Install **endpoint protection** software on all devices. Some examples include Trend Micro, Sophos, and Windows Defender. There are special endpoint security apps for phones and tablets. Lookout is an example.

WHAT IS ENDPOINT PROTECTION?

Endpoints are the devices that staff use, including mobile phones, laptop computers, and desktop computers. They are the "endpoints" of the campaign's network, and staff are the "end users." Endpoint protection centrally controls and manages security on remote devices. It's especially important for campaigns that allow staff to "bring your own device" (BYOD), since the campaign needs to ensure that the device is secure, free of malware, and can be wiped if stolen or lost. Endpoint protection can also monitor the device to make sure software is up to date and detect new malware or potential threats. For many campaigns, this will feel like a big lift, but building it into your routine onboarding and investing some time upfront can save you a lot of grief later.

1. Use **mobile device management (MDM) software**, which monitors activity to ensure all devices comply with the mobile phone and user device security policies you have established for your campaign. Examples include VMware AirWatch, Microsoft InTune, and JAMF. GSuite and Microsoft Office 365 also include an MDM service.
2. Use advanced threat protection services that monitor and alert for malicious activity, such as CrowdStrike Falcon or Mandiant FireEye. Crowdstrike sometimes offers Falcon breach prevention service pro bono through the Crowdstrike Foundation, depending on the needs of your campaign and campaign finance rules.

STEP 6: Networks

Networks are the system of physical hardware, digital software, and their connections. They represent another target-rich environment for attack. Network security comprises everything from how devices communicate with one another to using cloud services for data storage.

1. **Embrace the cloud. Store data on cloud services, not on personal computers or servers.** Anything stored on a personal device faces higher risk than the cloud.
    - No one should have access to all files on the network; accounts with comprehensive administrator access should not be used for day-to-day work. Divide your file storage into department folders and grant access accordingly.

- Ensure **access to shared content is by invitation only.** Some file management services also allow for implementing expiration dates on invitations and access.
- Periodically audit what is being shared and with whom.

2. Have a **separate "guest" wifi** network for visitors and volunteers that limits their access to campaign resources. Try to purchase routers that offer a "guest profile" that will automatically segment your network.
3. When traveling, or before you set up your campaign office, avoid public wifi services as much as possible and use trusted wifi networks wherever possible. If you need mobile wifi, then try to provide campaign staffers with mobile wifi hotspots for tethering. Public wifi is often free and easy to connect with, but attackers can also use it to penetrate your hardware.
   - Where possible, staffers should **use a VPN** (virtual private network). VPNs help protect against intruders when on public wifi. Examples of VPN services include ExpressVPN or TunnelBear. Not all VPNs are created equal. Beware of free services: many are looking to take your data!
4. **Secure your browser.** PC Magazine ranked Chrome and Firefox as the two safest browsers in 2017. Regardless of what browser you use, keep it up to date.

WHAT ARE VPNs?

A virtual private network (VPN) is an encrypted "tunnel" for your Internet traffic, hiding it from intruders. Some offices use it as a way to log remotely into the office network, but this isn't very common for campaigns. Campaigns should consider having their staff use a VPN on computers and mobile phones if they often have to use public wifi or untrustworthy networks (which is sometimes the case for traveling staff or field offices).

1. You can take more advanced steps to protect your network, but they should be implemented by an IT professional. We would suggest you ask them to include the following:
   - **Set up a hardware firewall.**
   - **Encrypt your wifi connection** using the WPA2 or 802.1x security protocols (do not use WEP).

- Configure cloud-based web proxies to **block access to suspicious sites** from any campaign-owned device, no matter where it is. Service provider examples include Zscaler, Cisco Umbrella and McAfee Web Gateway Cloud Service.
- Have your activity logs stored on a cloud service provider such as LogEntries or SumoLogic.
- **Segment your cloud-based storage** so that not everything is stored in the same place. Opposition research, strategy memos, and personnel files should be kept in different folders, and access to those folders should be restricted to the people who really need them. Consider a different storage system entirely for your campaign's most sensitive information. Restrict access so that only key personnel can access it, and only when using specific devices. (For example, if you use Microsoft365 for your office suite and document storage, but your most sensitive documents on a Dropbox or Box account.) If a member of the campaign becomes compromised, this kind of segmentation can limit the damage.

2. **Train staff not to connect their devices to unknown ports or devices.** Don't use public chargers at airports or events. Don't accept free phone chargers or batteries at events (that free USB drive may be loaded with malware!).

Authors & Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to Debora Plunkett for leading the project and Harrison Monsky for writing the document. We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

Defending Digital Democracy
Eric Rosenbach, Co-Director, Harvard Kennedy School Belfer Center
Robby Mook, Belfer Center Fellow
Matt Rhoades, Belfer Center Fellow
Heather Adkins, Director, Information Security and Privacy, Google
Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike
Josh Burek, Director of Global Communications and Strategy, Harvard Kennedy School Belfer Center
Chris Collins, Co-Founder, First Atlantic Capital
Caitlin Conley, student, Harvard Kennedy School
Mari Dugas, Project Coordinator, Defending Digital Democracy, Harvard Kennedy School Belfer Center
Josh Feinblum, student, Massachusetts Institute of Technology
Siobhan Gorman, Director, Brunswick Group

Stuart Holliday, CEO, Meridian International Center
Dai Lin, student, Harvard Kennedy School
Kent Lucken, Managing Director, Citibank
Katherine Mansted, student, Harvard Kennedy School
Nicco Mele, Director Harvard Kennedy School, Shorenstein Center
Debora Plunkett, former Director of Information Assurance, National Security Agency
Jim Routh, Chief Security Officer, Aetna
Suzanne E. Spaulding, Senior Adviser for Homeland Security, Center for Strategic and International Studies
Matthew Spector, student, Harvard Kennedy School
Alex Stamos, Chief Security Officer, Facebook
Phil Venables, Partner and Chief Operational Risk Officer, Goldman Sachs

Additional Authors and Contributors
Ryan Borkenhagen, IT Director, Democratic Senatorial Campaign Committee
Michael Chenderlin, Chief Digital Officer, Definers Public Affairs
Robert Cohen, Cyber Threat Analyst, K2 Intelligence
Julia Cotrone, Special Assistant, Definers Public Affairs
John Flynn, Chief Information Security Officer, Uber
Daniel Griggs, Founder and CEO, cmdSecurity Inc.
Eben Kaplan, Principal Consultant, CrowdStrike
Greg Kesner, Principal, GDK Consulting
Ryan McGeehan, Member, R10N Security
Jude Meche, Chief Technology Officer, Democratic Senatorial Campaign Committee
Eric Metzger, Founding Partner and Managing Director, cmdSecurity Inc.
Zac Moffatt, CEO, Targeted Victory
Harrison Monsky, student, Harvard Law School
Colin Reed, Senior Vice President, Definers Public Affairs
Jeff Stambolsky, Security Response Analyst, CrowdStrike
Frank White, Independent Communications Consultant
Sally White, student, Harvard University
Rob Witoff, Senior Security Manager, Google

Belfer Center Web and Design Team
Arielle Dworkin, Digital Communications Manager, Harvard Kennedy School Belfer Center
Andrew Facini, Publications and Design Coordinator, Harvard Kennedy School Belfer Center

Downloads

Cybersecurity Campaign Playbook [PDF]

Handout For Staff Members [PDF]

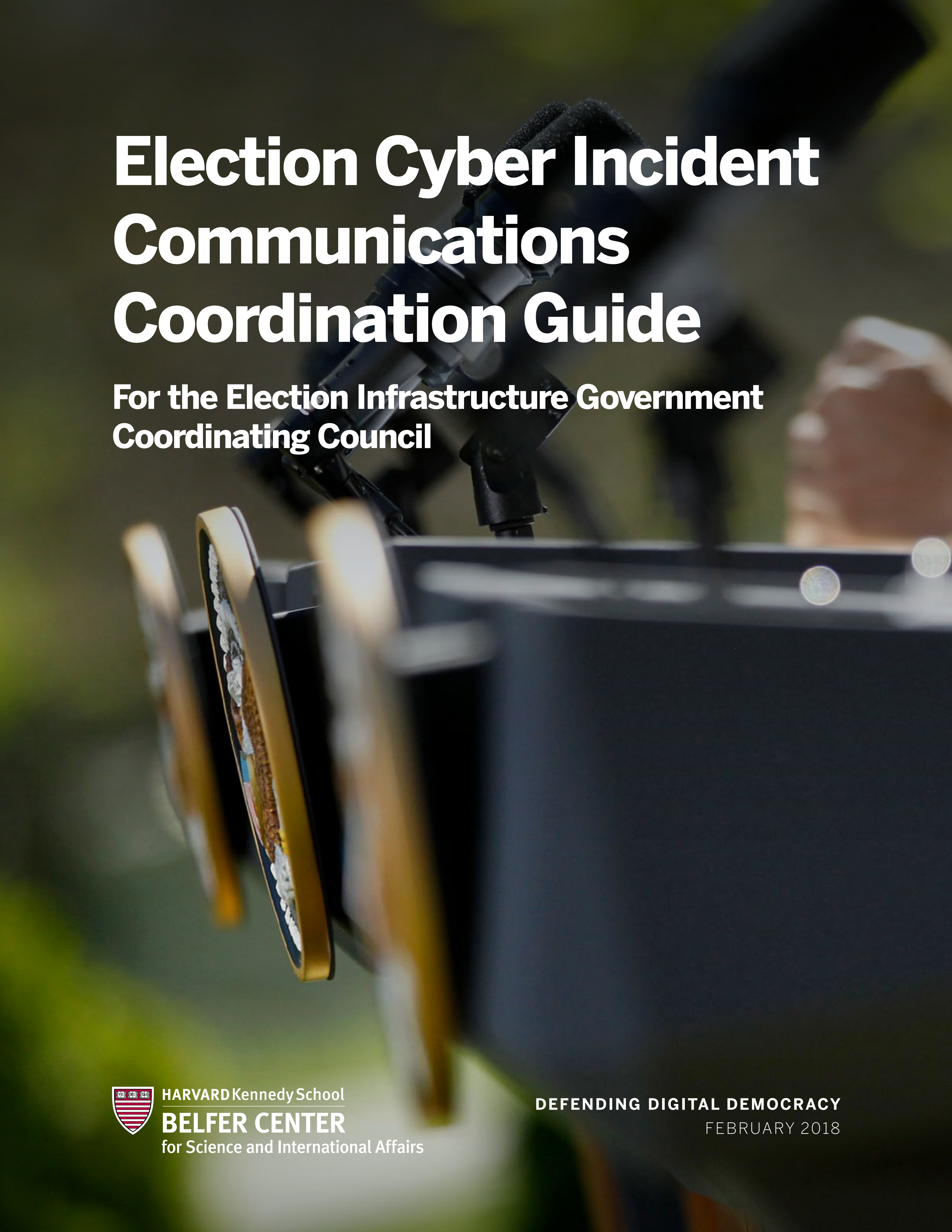
Handout For Family Members [PDF]

For more information on this publication: Please contact the Belfer Communications Office
For Academic Citation: "Cybersecurity Campaign Playbook." Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2017.

Harvard Kennedy School Belfer Center

Election Cyber Incident Communications Coordination Guide

February 2018



Election Cyber Incident Communications Coordination Guide

For the Election Infrastructure Government Coordinating Council

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Cover photo: A view of the podiums during a news conference in the Rose Garden at the White House, Monday, April 2, 2012. (AP Photo/Charles Dharapak)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Election Cyber Incident Communications Coordination Guide

For the Election Infrastructure Government Coordinating Council

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help secure democratic elections against cybersecurity threats and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals.

Now, we are releasing a set of three playbooks designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is the Coordination Guide.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors. To better understand the cyber threat and other challenges that election administrators face, our team spent four months interviewing state officials about their communications practices and how they would or would not apply these practices in a cyber incident. We spoke with state and local election officials, as well as key national-level players and members of the Election Infrastructure Government Coordinating Council (EI-GCC).

These interviews exposed the range of challenges election officials confront in the cyber domain. One of the most significant needs we encountered was the ability to communicate consistently across states in the event of a major election cyber incident, in order to maintain public trust.

This Guide is primarily intended for use by the EI-GCC to coordinate multiple voices (and multiple facts) in an election cyber incident that crosses traditional jurisdictions. We are releasing the Guide publicly, because a range of officials may be interested in learning more about how state and local leaders can, and should, coordinate their communications in the event of this type of cyber incident. We hope this Guide becomes a starting point for the EI-GCC to establish its role as a central communications node in the event of an election cyber incident.

Finally, we would like to thank the election officials around the country for whom we wrote this guide You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Siobhan Gorman** for leading the project and who, in addition to **Matt Chandler**, **Meredith Davis Tavera**, and **Chris Farley**, wrote this Coordination Guide.

We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Lori Augino, Director of Elections, WA Office of the Sec. of State

Matt Chandler, Partner, Frontier Solutions

Caitlin Conley, Executive Director, D3P

Amy Cohen, Executive Director, National Association of State Election Directors

Meredith Davis Tavera, D3P, Harvard Kennedy School

David Forsey, Policy Analyst, National Governors Association

Shannon Cortez, Deputy Director of Elections, WA Office of the Secretary of State

Chris Farley, Associate, Albright Stonebridge Group

David Forsey, Policy Analyst, National Governors Association

Karen Ejiofor, Staff Assistant, Belfer Center

Siobhan Gorman, Director, Brunswick Group

Eben Kaplan, Principal Consultant, CrowdStrike

Jane Khodos, Senior Director, Comms. and Content, FS-ISAC

Matthew Masterson, Commissioner, Election Assistance Commission

Jeff McLeod, Division Director for Homeland Security and Public Safety, National Governors Association

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Michelle Tassinari, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of MA

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

How to Use this Communications Guide

This communications guide includes best practices and guidelines to help the Election Infrastructre Government Coordinating Council (EI-GCC) quickly coordinate the response to an election-related cyber incident that affects more than one state during the early days of the incident. While every cybersecurity incident is unique, this document provides a foundation on which the EI-GCC can build a response that addresses the incident with the goal of maintaining confidence in the election system.

This Guide should be owned by the communications director, or a similar position, at the EI-GCC and be updated at least annually.

Key topics include:

Strategy, Mission, and Objectives: The purpose of the Guide is to help election officials maintain public confidence in the integrity of the U.S. election system in the event of an election-related cybersecurity incident.

Establishing a Cyber Communications Baseline: This section explains the importance of educating the public and other key stakeholders on cyber threats facing the election process and steps currently being taken to counter them.

Cyber Incident Best Practices: This section includes best practices for communicating with the media and other key stakeholders.

Communications Process Workflow: This component includes diagrams that outline who will manage the cyber crisis communications response and serve as spokesperson during an incident.

Response Checklist: This checklist broadly outlines steps that should be taken during the first several days after learning about a potential incident.

Executive Summary and Purpose

What constitutes a "cyber incident" in elections can range from theft of voter registration data to disruption or manipulation of the vote tally. This Guide is designed to help coordinate and align communications across jurisdictional boundaries in an election-related cybersecurity incident that involves more than one state. Its primary purpose is to maintain (or regain) public confidence in the face of such an incident.

This Guide is written to help the Election Infrastructure Government Coordinating Council (EI-GCC) assist state and local election officials, who will need to communicate across jurisdictions if an election-related cyber event has impacts beyond a single state. While every jurisdiction should have its own plan to respond to a cyber incident, many incidents will have implications beyond state boundaries. It is critical to coordinate the response from the outset, so public comments confidently convey that the issue is being addressed and maintain public trust in election systems across the country.

We recommend the creation of a communications coordination structure within the EI-GCC, including a communications director, or similar role, who would be a key spokesperson in a cyber crisis.

A multistate cyber incident could take many forms. It could be a series of incidents that collectively have a broader impact. It could be one or a few incidents that, because of their strategic significance or other factors, have an impact beyond state boundaries, or receive outsized attention from national media outlets. This could even be a false rumor that requires a coordinated effort to stamp it out.

This Guide provides:

1. A set of best practices for communicating about an election-related cyber incident
2. A process for coordinating multistate communications decision-making, including spokespeople and communications messages

Additional communications response materials, including a sample escalation process and scenario-planning materials, are available to election officials and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

Strategy, Mission, and Objectives

The potential for cyberattacks on our elections systems is an unfortunate reality of our time. Election officials should recognize, and plan for, a possible incident. **The primary objective of this communications guide is to enable the EI-GCC to help election officials maintain public confidence in the integrity of the U.S. election system** in the event of cyber incidents both locally and crossing state boundaries.

Election officials from both parties and at all levels of government agree that there is a shared national interest in preserving the public trust in our election system.

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible, especially in today's perpetual cycle of traditional and social media coverage.

Maintaining public trust is most effectively accomplished when election officials—across parties and jurisdictions—speak with one coordinated voice. If federal officials are contradicting state leaders, as occurred in 2016, the public is left confused and it can become all the more difficult to maintain confidence in the election process. Likewise, if federal, state, or local officials are contradicting one another, it is counterproductive and confusing to the public. For these reasons, EI-GCC will play a crucial role in coordinating the response.

All public statements should demonstrate the incident is being handled competently. Any specifics that are provided should be limited only to those that will not change. The scope of the incident, for example, is likely to shift and shouldn't be discussed publicly at the outset. Modifying your story can undermine confidence in the management of the incident and the election system itself.

To institutionalize a means to maintain public trust, **the communications response strategy underlying this Guide coordinates communications messages and delivery among election officials in a multistate cyber incident** to ensure consistency and accuracy of public information. To enable a unified response, we provide communications best practices and coordination processes.

Elections are governed at the state and local level, and there is a national interest in maintaining the integrity of, and confidence in, our elections system. So it is important to have a process that will enable officials from all levels of government to: obtain and analyze the information; decide who will speak about the national implications of the incident; and provide information and communications to all elections officials, so they can communicate accurately, dispel rumors, and reinforce coordinated messages.

Beyond the coordinated multistate process outlined in this Guide, election officials at all levels of government should take measures to prepare for a cyber incident.

Among the steps you can take immediately are:

- **Establish (or update) a state or local communications response plan** to an election-related cyber incident. For a template state or local cyber communications plan please see the Election Cyber Incident Communications Plan Template.

- **Ensure that the communications plan is aligned** with the corresponding technical response plan, and that both are regularly updated.

- **Test those plans** with simulations.

- **Obtain regular updates** on cyber threats, particularly as they relate to elections.

- **Maintain relationships with officials** who will be relevant to coordinating a response to any cyber incident, including federal officials at the local level and other local community leaders.

- **Coordinate with political parties.** It is much easier to agree to protocols for sharing information about and responding to a cyber incident before the incident and before an election.

- **Educate the public about the work you are doing.** Set the expectation that there will likely be some cyber threat activity during an election and explain how that activity differs from what would be required to interrupt the elections process.

It is important to update and exercise communications response plans frequently—at least every year—to familiarize new players with the process and ensure you apply lessons learned from past experiences and exercises.

Establishing a Cyber Education Baseline

The public needs to understand the steps state elections officials are taking to counter cyber threats, as well as how difficult it is to execute a cyberattack that will disrupt an election outcome. If the public, and the media, understand the "new-normal," baseline activity of cyber threats targeting elections, they will be less likely to worry unnecessarily about news of small-scale election-related cyber incidents. If you don't have to spend considerable time allaying concerns over inconsequential incidents, you can focus your attention on the consequential ones.

The main point to make is that cyberattacks are now an issue all election officials must contend with, and the states have taken, and continue to take, steps to mitigate those threats. However, not every attempt is successful, and even successful ones are very unlikely to impact the outcome of an election.

Communications in a cyber crisis are most effective when the public has a baseline understanding of:

- The continuing work at all levels of government to counter that malicious activity and try to ensure it does not escalate to a major cyber incident
- The nature of the election data your agency holds, most or all of which is public data
- The malicious, but inconsequential, cyber activity that takes place regularly

We recommend that the EI-GCC consider taking on some of this public education role, which would address issues that extend across the states. The council is in a strong position to draw on data from across the country and across levels of government about both threats and actions being taken to enhance the cyber defenses of election systems. For this reason, we suggest that it consider publishing an annual report on the state of election cybersecurity.

The EI-GCC, perhaps in concert with the relevant associations and Information Sharing and Analysis Centers, could provide a regular cadence of cyber threat information, so the public understands how frequently attempts are made by a range of cyber threat actors to target election infrastructure. Making this information common knowledge will mitigate the tendency to treat every reported attempted attack as a reason to question the election system.

The type of information you may want to share could include statements such as: "Based on threat information from the Department of Homeland Security and the Federal Bureau of Investigation (or state/local law enforcement), we are taking the following steps to address and mitigate these threats." If appropriate, this effort could take the form of regular background briefings for the media, as well as online materials and public panels or other educational events for other key stakeholders. The EI-GCC could also consider a joint public panel or forum with representatives of both political parties to discuss measures states are taking to mitigate cyberattacks.

The EI-GCC should also consider sharing limited, aggregate information on successful attacks once they have been addressed, which would establish the EI-GCC as a valuable resource for this type of information.

You should couple the cyber threat data with information on the actions states and localities are taking to strengthen the cyber defenses of election systems. This information should be specific enough to be credible while not being so detailed as to undermine your defenses. Work closely with information security and legal experts to strike the right balance.

We discuss how to establish a communications baseline in more detail in the section on communications process on Page 15.

Cyber Crisis Communications Best Practices

Election-related incidents fall broadly into five categories:

- Online rumors that seek to undermine confidence in an election
- Reconnaissance of election-related systems
- Theft of voter or other election data
- Data manipulation that could affect an election outcome
- Data destruction

The top priority in a cyber crisis will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly. To do this, the EI-GCC will need to prepare, train for, and test its response ahead of time—especially because it is a new organization.

Planning Ahead

Near-term Planning	Longer-term Planning
• **Determine internal roles and responsibilities**. Make sure there is a clear escalation process for the EI-GCC and the right teams are talking to each other in the event of a cyber incident. Make an individual responsible for ensuring that this process is established and updated. • **Assess the current crisis communications plan** and analyze communications gaps and weaknesses. • **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials. • **Ensure that cyber incident response is part of the operational continuity plan**. Make sure there is a backup communications plan and system in place.	• **Conduct crisis simulation and table-top exercises**, coordinated with legal, technical, and outside advisors, including key senior leaders from multiple states, counties, coordinating bodies, and the federal government. • **Conduct stakeholder mapping and a risk analysis** to understand risks to trust in the election system, priority stakeholders, and how to reach stakeholders to address key concerns. Pay particular attention to outreach to voters and political parties. • **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats. • **Educate the public** through online channels and public events on the resiliency of the election system and the current work to mitigate cyber threats.

Communications Response

Best Practices

Be transparent but careful. Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously, but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident.

Focus on actions you are taking to address the issue. To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and address any broader risks to the system.

Provide context. In an election-system incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

Be visual. Cybersecurity can be challenging to understand depending on a person's technical background. The quickest way to get your message out is to pair it with a graphic. Connect with design teams who can provide you infographics and develop a library of graphics and photos you can draw from.

Use the right digital tools. Use social media to dispel rumors. When a cyber incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation and inaccuracies.

Learn from the incident. Use your and others' experiences to improve your cybersecurity practices and crisis plans.

Guidelines for Communicating with the Public

Focus your communications on your most important stakeholder—the public. You will be tempted to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this given situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify cybersecurity issues whenever possible.

Demonstrate transparency by communicating with the public on a regular basis. Establish a regular series of communications with the media and the public about the cybersecurity measures you are taking now, so that the first time they hear from you is not in a crisis.

Best Practices for Countering Misinformation

Establish the facts, and double-check them. You need to ensure that you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to be certain that you do not accidentally provide misleading information.

Develop a simple, accurate, short counter-message. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later.

Respond quickly. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready to disseminate as soon as possible.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Demonstrating transparency can help to counter false claims. Opportunities to demonstrate transparency could include inviting reporters "behind the scenes" at a polling place.

Engage on all platforms. Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms.

Avoid repeating misinformation. Focus on providing accurate facts and do not repeat the false messages. For example, if false rumors circulate that lines at the polls are many hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

Communications Process

Maintaining a coordinated process is critical to effective and efficient communications planning and response to a cyber-related incident. For an incident affecting multiple states, this coordinated communications process outlines:

- Key stakeholders
- Phased planning and response
- Coordination functions
- Feedback loop to incorporate lessons learned

In this communications process, we assume that information and messaging coordination functions will be performed by cross-jurisdictional organizations that have played a similar role in past crises. Further, we recommend that new coordinating functions and mechanisms be created to execute information-sharing and communications.

We recommend that the EI-GCC—with support from other interested parties, such as the National Association of Secretaries of State (NASS), International Association of Government Officials (IGO), the U.S. Election Assistance Commission (EAC), the National Association of State Election Directors (NASED), and the National Governors Association (NGA)—establish a Cybersecurity Communications Response Group (CCRG).

This newly formed entity will provide the EI-GCC and its stakeholders with a communications coordination function that currently does not exist, allowing for collaborative, coordinated public message planning and execution if and when it is needed in the future.

Phase 1: Baseline Communications Activities

On a regular basis, the CCRG will provide updates to the public and other key stakeholders on current cyber threats and actions being taken to counter them. These baseline updates, whether part of a regular cadence or spurred by suspected nefarious activity, should be developed and coordinated with the expectation that they will be made public. Audiences and stakeholders are catalogued below with recommendations for actions that can be taken now to establish or maintain relationships with them.

Communicating with these groups on a regular basis, before something happens, is key to setting a baseline with critical audiences so that there is a level of understanding around the issue that allows mutual alignment on escalation and coordinated response. In order to provide this ongoing education, we recommend communicating early and often, in addition to when moments of interest (i.e., elections) arise. This baseline work could take the form of behind-the-scenes demonstrations and briefings for your audiences.

Stakeholders may include:

State / Local Comms. Counterparts

Law Enforcement

Federal / State Lawmakers

Media

Interested Parties

State and Local Communications Counterparts: Knowing your state and local counterparts is key to the planning and response actions discussed in later phases. The EI-GCC should maintain a "living list" of communications officials and accurate contact information, so these individuals can be reached on short notice for incident coordination and planning.

Law Enforcement: In the event of a cyber incident, federal, state, and/or local law enforcement will be involved in the response. Creating and maintaining relationships with key law enforcement officials and associated communicators in law enforcement agencies ensures more seamless coordination and information-sharing before, during, and after an incident.

Federal/State Lawmakers: Federal and state lawmakers play an important role in authorizing and overseeing election and cybersecurity measures. They also are likely to speak publicly about an election-related cyber incident, so communication with them is critical before, during, and after an incident. Not only are lawmakers beneficiaries of a safe and secure elections system, but they have a vested interest in maintaining the public's trust in that system. Communicators should build relationships with key figures in Congress and statehouses, including their respective communications staffs, in advance.

Media: The media is a key information conduit to voters, providing news and commentary that shapes and defines public opinion and a belief in the election system's integrity. Establishing ongoing relationships with key reporters who cover both cybersecurity and election-related issues at the national, state, and local level will be important in shaping accurate coverage throughout all phases of cyber-related preparation and response.
You should focus on two categories of media:

- **Traditional Media—**Mainstream outlets and reporters;
- **Influencer Media—**This category includes influential bloggers, outlets, and commentators, as well as outlets likely to reach them.

Interested Parties: You should develop relationships with voting advocacy and other third-party groups, because they play a role in maintaining the public's confidence in elections. Political parties an campaigns are a critical group with which you should develop a trusted relationship in advance. Third-party groups may also include vendors, researchers specializing in elections, technology service providers, or other industry service providers. We recommend as a next step that the CCRG develop an initial list of key groups, which should be maintained and updated by the team lead.
This list could include:

- **Political Parties and Campaigns**
- **Election Groups**
- **Think Tanks**
- **Academics**

Phase 2: Communications Planning, Activation, and Coordination

Cyber-related incidents rely on evolving investigations, making their scope and impact difficult to understand, particularly at the outset. This can make communications decision-making, coordination, and messaging even more important for reducing confusion.

Some incidents may be discovered as an attack or breach occurs, while most tend to be discovered after the fact—often after significant time has passed. The key to an effective response is not just coordination but also knowing with whom to coordinate. In any response, there are likely to be multiple voices speaking publicly, at both the national or field level.

In this phase, we assume an anomalous event has been identified, which activates a communications coordination scheme. It may be detected by a range of entities, such as a security researcher, state/local election official, law enforcement, or media.

When an incident occurs, many representatives from a variety of organizations will become involved. The section below outlines resources, coordination mechanisms, lines of coordination, and a checklist to be used in response to, or in advance of, a cyber-related incident.

Assembling Key Players

Note: *The U.S. Federal Government's National Response Framework outlines public information as an Emergency Support Function (ESF) and includes a framework for public information coordination and action around incidents that involve, or may involve, federal response. This process aligns with the ESF #15 Standard Operating Procedure.*

CCRG Roles & Responsibilities: The CCRG should establish the following roles for responding to a multistate cyber incident. These individual roles can be filled by specific people from a variety of interested parties, which may include, but are not limited to, NASS, NASED, IGO, EAC, and NGA.

Please note that as the EI-GCC builds on this Guide, updates should include a table with these roles assigned to individuals, along with their contact information.

Communications Director–On behalf of the EI-GCC, oversees the functional coordination resources, processes, and staff. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with EI-GCC and interested parties. The communications director position can be filled by different people on a rotating basis; for example, the EI-GCC could designate a communications director to stand duty quarterly. The role should be filled by a senior communicator from the EI-GCC participants or other interested parties and have the relevant management, crisis, and media operations experience to understand not only their role but also the other roles outlined as part of the CCRG.

Affected Community Communications Representatives–Usually senior communicators from affected state or local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process. This may include a communicator from the governor's office and/or communicators from state and/or local elections offices.

Media Operations Director–Responsible for communication with reporters and for media monitoring on behalf of a multi-state communications coordinating body. Oversees near-term, "24-hour" communication operations, i.e., execution of communication plans.

Social Media Director–Responsible for online communications via ESCC web platforms, as well as coordination with interested parties' digital media teams in order to promote and cross-promote content.

Communication Plans Director–Responsible for forward-looking communication plans beyond the immediate "24-hour" period.

Congressional/Inter-governmental Affairs Liaison–Responsible for coordinating congressional/governmental briefings for members of Congress, state legislatures, or other elected officials with communications staff. Coordinate through the Affected Community Communications Representative, who is likely to be a member of the ESCC or interested parties' government affairs team.

Law Enforcement Affairs Liaison–Responsible for coordinating communications information with law enforcement and affiliated communicators.

Technical Liaison–Responsible for being the conduit of technical information between operational and communications teams. Ensures accuracy of technical data being released by communications team and serves as subject-matter expert for all such information.

Activation of the CCRG: The CCRG, while regularly communicating in Phase 1 during baseline operations, should plan for and exercise the activation of the CCRG in a crisis. Activation of the CCRG would be at the discretion of the Communications Director, with input from operational leads in response to a verified or potential incident. Additional information on the escalation process is in the Appendix available to election officials and can be obtained upon request from NASS, NASED, or the EAC

Generally speaking, this activation would be executed via a blast email to CCRG members with shareable background information on the incident, direction on the use of coordination mechanisms (discussed below), and next steps. For example, on discovery of a potential incident, the Communications Director would activate the CCRG by hosting an Election Sector Incident Communications Coordination Line call regarding the incident, thereby beginning the communications coordination process.

Election Sector Incident Communications Coordination Line (ESICCL): This bridge line is a standing conference call line that can be created to use for coordination before, during, or after a cyber-related incident. The CCRG will maintain a list of relevant contacts from federal, state, and local election offices in order to invite relevant parties to a call, should it be necessary. This resource does not currently exist and it would be incumbent upon the CCRG to coordinate the creation of this standing line at the outset.

Election Sector Information Center (ESIC): In the event of a multistate event, the CCRG should create a specific Information Center where communications activity is planned, coordinated, and executed real-time. This should include all the roles above and can reside in one physical location or it could be done virtually through online means. An ESIC would be the functional nerve center of all communications-related activity.

Using the Election Sector Incident Communications Coordination Line (ESICCL)

As the standing conference call line for election sector cyber-related incidents, the ESICCL can be a key coordination mechanism for communicators to share both operational data, as well as coordinate messaging and communications-related activity.

Upon the activation of the CCRG, the Communications Director will stand up the ESICCL and distribute the time and conference line to invited participants for an initial conference call. This call could include representatives from affected communities, as well as the CCRG roles listed above and any other CCRG participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by Communications Director for CCRG
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by EI-GCC Representative
- Conclusion and next steps

Standing up the ESIC

Should an event rise to the level where ongoing, real-time coordinated public information flow is necessary, the CRCG could stand up either an in-person or virtual ESIC where personnel could work together.

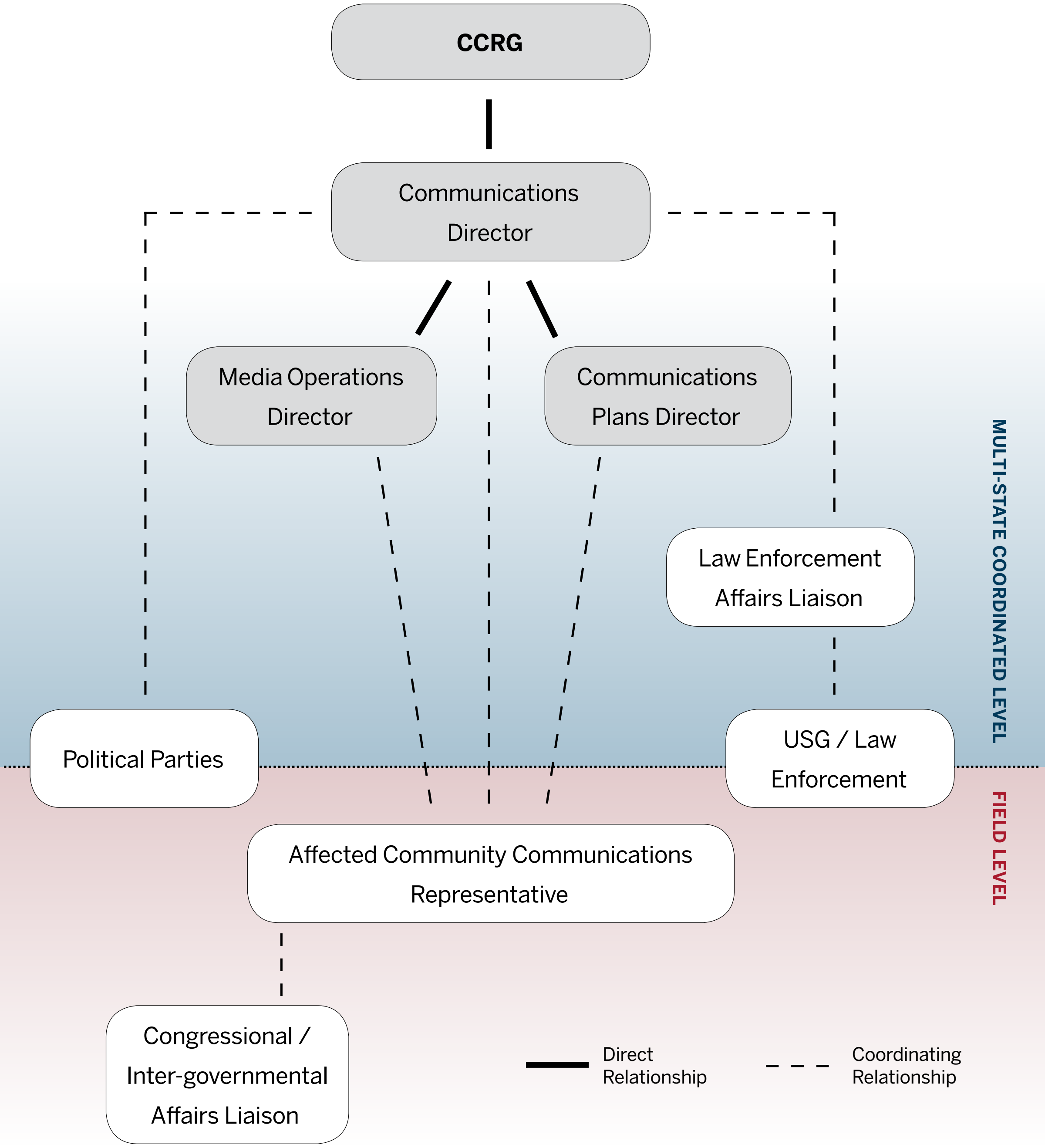
The ESIC would be stood up by the Communications Director, who would make a determination as to the critical personnel needed, as well as the location/online.

The CRCG, as part of steady-state planning, should identify both likely and convenient physical locations where an ESIC could reside should it be needed, as well as functional online collaboration tools to use in the event of a remote ESIC. In general, it is advisable to co-locate the ESIC with any space that is being used to coordinate operational response activity.

Current Coordination Processes

Should there be current coordination processes that are effective in sharing information, such as regular calls or email listservs, continue to use them—particularly prior to, or during the beginning phases of, activation. However, the scope and volume of an incident may make more direct communications, such as via the ESICCL or ESIC, more useful.

Lines of Coordination

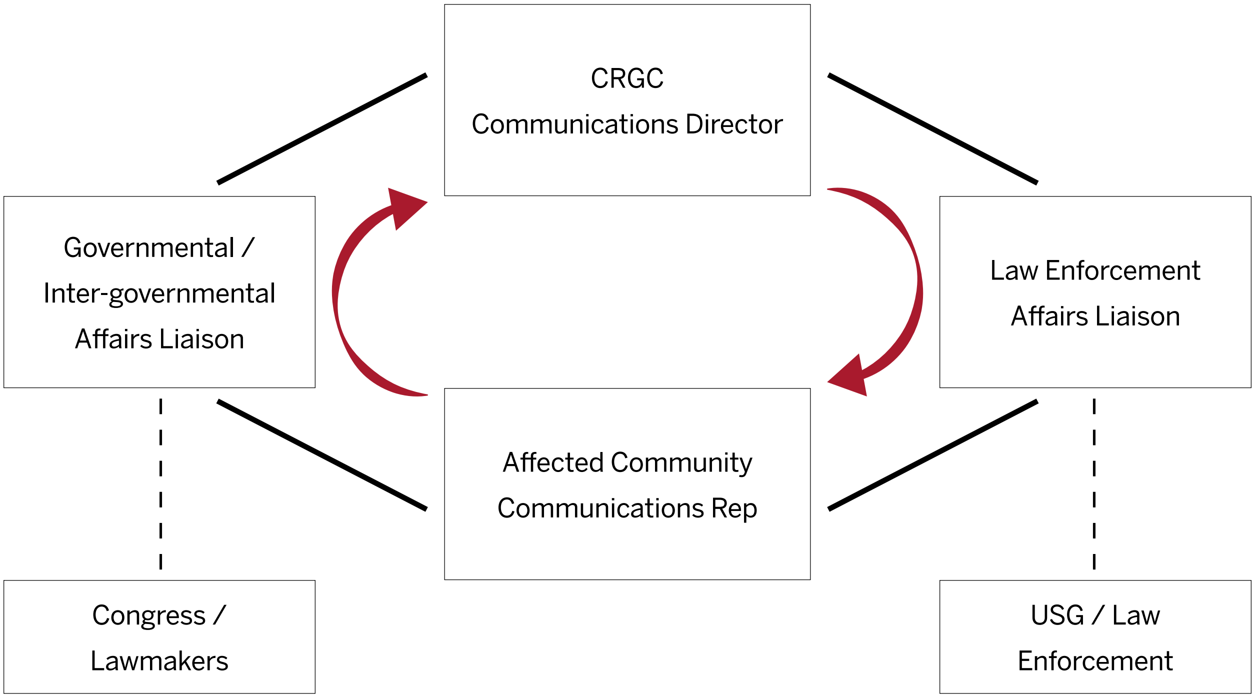

CCRG
Communications Director
Media Operations Director
Communications Plans Director
Law Enforcement Affairs Liaison
Political Parties
USG / Law Enforcement
Affected Community Communications Representative
Congressional / Inter-governmental Affairs Liaison
Direct Relationship
Coordinating Relationship
MULTI-STATE COORDINATED LEVEL
FIELD LEVEL

Phase 3: Message/Document Drafting, Coordination, and Distribution

Message/Document Drafting and Coordination

It is best to have some communications materials ahead of time; however, every incident is different and depends on a range of factors, so communicators will oftentimes have to adapt on the fly.

Messaging will need to be adapted, drafted, coordinated, and distributed quickly in order to effectively respond. In addition to the coordination resources, mechanisms, and processes described above, the diagram below shows how that loop may work practically, in and among the various parties who will be speaking publicly.

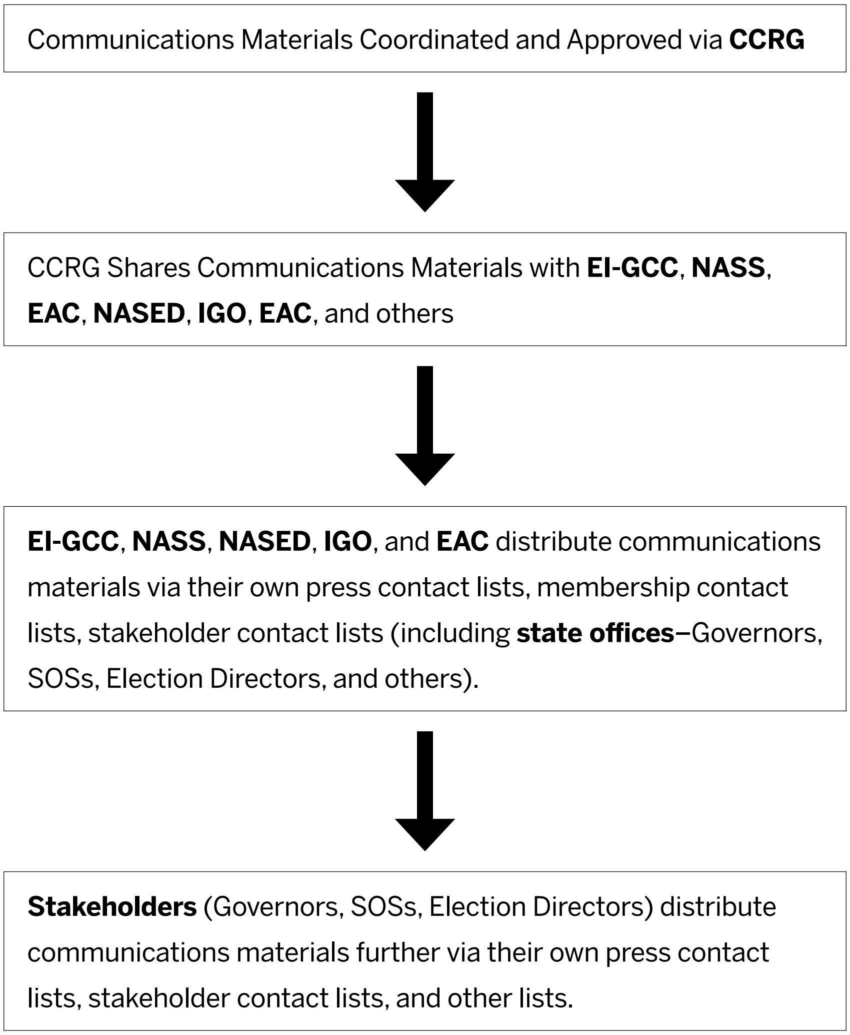

CRGC
Communications Director
Governmental / Inter-governmental Affairs Liaison
Law Enforcement Affairs Liaison
Affected Community Communications Rep
Congress / Lawmakers
USG / Law Enforcement

The CCRG staff will not necessarily retain authority to approve messages emanating from affected communities' communications staffs, nor vice versa; however, the CCRG staff can provide message guidance when needed or warranted. In addition, key inputs should be sought from Congressional/Inter-governmental Affairs and Law Enforcement Liaisons, and approval authority can be retained by those communicators with whom these liaisons work at their home agencies or organizations.

Distribution

Distribution of approved communications materials to the public and other stakeholders should leverage, and mirror, existing processes to the degree possible. The CCRG, by virtue of its makeup, with communications professionals from a variety of relevant organizations, should coordinate the messaging, but largely leave distribution to the organizational members.

A sample distribution process is illustrated below:



Communications Materials Coordinated and Approved via **CCRG**

CCRG Shares Communications Materials with **EI-GCC**, **NASS**, **EAC**, **NASED**, **IGO**, **EAC**, and others

EI-GCC, **NASS**, **NASED**, **IGO**, and **EAC** distribute communications materials via their own press contact lists, membership contact lists, stakeholder contact lists (including **state offices**–Governors, SOSs, Election Directors, and others).

Stakeholders (Governors, SOSs, Election Directors) distribute communications materials further via their own press contact lists, stakeholder contact lists, and other lists.

Phase 4: Evaluation and Feedback

Incorporating both real-time evaluation and feedback, as well as post-incident after-action reviews into your response is critical to both the response you are currently managing, and capturing lessons learned for the future.

Real-Time Evaluation

While capabilities and resources may differ greatly among affected communities, the CCRG could augment these by providing services that can assist the holistic communications response, including:

> **Media Monitoring**–It is critical to understand how the media tone is shaping up. Media monitoring should be compiled at least daily, providing insight on tone and volume and identifying areas for further concentration or strategic/tactical communications changes.

> **Social Media Analysis**–Similar to traditional media monitoring, social media listening tools and analysis can provide key insight into which messengers are driving conversation about the incident, as well as how voters are reacting to news and sharing information.

> **Call Center Analysis**–If the affected community has a voter call center, it is important to track and analyze the questions and comments received. This information can be a key indicator of misinformation or provide insight into where efforts need to be expanded to get accurate information to voters.

> **Polling/Public Opinion Research**–In order to gain more in-depth insights, polling or public opinion research can do much in terms of uncovering voter reactions to an election-related cyber incident, helping shape near and longer-term strategy.

After-Action Review and Report

Once an incident has concluded, it is important to review communications-related activities, discuss what worked and didn't work, and document those lessons to be incorporated into both steady-state and crisis planning.

Many of the coordination resources and mechanisms described above can be adapted for this purpose, for example the ESICCL call. The after-action process should analyze the incident from start to finish, examining the Plan-Prepare-Respond-Recover communications lifecycle of that incident.

Your after-action report should include:

- A summary of the incident;
- an overview of the operational response;
- the communications objectives;
- and by phase, with specificity:
  - concern
  - outcome
  - recommendations

This after-action process will assist in building your communications response capability and coordination in a resilient process that can be more effectively utilized when facing future incidents.

Communications Coordination and Response Checklist

This checklist will help guide actions prior to, and through, the first several days of a multi-state election-related cyber incident.

There are five lists:

- 🟦 **Before a cyber crisis**
- 🟥 **Before a cyber crisis becomes public**
- 🟨 **Multistate Election-Related Cyber Incident Assessment & Activation**
- 🟧 **Coordination/Communications Outreach**
- 🟩 **Products**

🟦 Before a cyber crisis

□ Identify office protocol and a crisis communications team. (Should include IT).

□ Create a list of terms with common nomenclature for use by all stakeholders.

□ Set an internal communication plan with elections staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for disseminating information and interfacing with the public/media.)

□ Ensure that all stakeholders can be reached in a crisis without access to networks or smart phones.

□ Craft communications materials that can be used in a potential cyber incident. (For examples, elections officials may request sample materials from NASS, NASED, or the EAC.)

□ Ensure that staff understand their role in a cyber incident. For those who do not have a specific role, ensure they understand why their work matters to the outside world and how they can continue doing their jobs while designated managers handle the cyber incident.

□ Ensure that communications plans can be accessed and are regularly updated.

Before a cyber crisis becomes public

- □ Obtain technical briefing. (Assess and verify all information.)
- □ Decide whether to activate CCRG.
- □ Decide whether website can remain online. If you must disable it, launch a microsite (hosted on a different network) in its place.
- □ If email is potentially compromised, use an outside communications channel.
- □ Consult authorities, if needed.
- □ Meet internally in war room; set internal communication schedule.
- □ Determine CCRG roles and responsibilities, if you have not done so already.
- □ Assess stakeholders.
- □ Determine broad communications strategy.
- □ Prepare holding statement.
- □ Develop communications plan.
- □ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).
- □ Establish plan for traditional and social media monitoring.
- □ Establish media response protocol.
- □ Notify affected employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- □ Notify stakeholders (See list on reverse page), if appropriate, and galvanize support.

Multistate Election-Related Cyber Incident Assessment & Activation

□ Notification to, and activation by CRCG, of a cyber-related incident or threat.

□ Situation Assessment/Escalation.

  □ **High-Intensity Incident**: Cyber-related incident that triggers reporting obligations, or one that is highly visible requiring response.

  □ **Medium-Intensity Incident**: Cyber-related incident resulting in the loss or compromise of the data or systems, but no formal reporting obligations are triggered. There may be some awareness of the incident, however, spurring proactive communication.

  □ **Low-Intensity Incident**: Cyber-related incident resulting in minor disruptions that may not be visible to public.

□ If Major or Moderate, Media Operations Director and Communication Plans Director identified by Communications Director.

□ Additional Relevant Personnel identified.

□ Contact information for Relevant Personnel distributed.

□ CRCG designates spokesperson, if applicable.

□ Depending on assessment of situation, key messages determined based on specific scenario.

Coordination/Communications Outreach

- □ Communications Director activates ESICCL call.
- □ Incident Overview.
- □ Affected Communities Communications Representative Update.
- □ Initial Response Communications Plan.
  - □ Designate spokesperson based on type of incident, geography(ies) affected, and scope. In a Major Incident, the spokesperson role may include several people including a EI-GCC representative as well as an Affected Community spokesperson as well to share information at both a field and national level. In a Minor Incident, a single spokesperson may suffice, i.e. an Affected Community spokesperson.
  - □ Prep designated spokesperson for media engagement. This includes review of relevant facts and messaging as well as a peer review session, known as a "murder-board."
- □ Congressional/Inter-governmental Affairs Update.
- □ Congressional/Inter-governmental Affairs activity and plans.
- □ Law Enforcement Liaison Update.
- □ Law Enforcement Liaison activity and plans.
- □ Messaging Coordination outlined by Communications Director.
- □ Battle Rhythm (Daily Schedule).
- □ Conclusion & Next Steps.
- □ Communications Distribution & Rollout.
- □ ESIC activation, if necessary.

Products

- □ Staffing Plan with updates for Communications Director.
- □ Battle Rhythm (Daily Schedule).
- □ Staffing Matrix and Organization Chart.
- □ Communications Plan.
- □ Advisories.
- □ Press Releases.
- □ Traditional and Social Media Monitoring Reports.
- □ Regular/Daily update on response activities.
- □ Blog and Social Listening Updates.
- □ Talking Points.
- □ Website updates.
- □ Congressional/Inter-governmental Advisories, fact sheets, operations reports and briefing materials.
- □ Daily Communication Summary to include next day activity plans.

Conclusion

As we head into the next election cycle, we hope that this Guide provides additional tools to help the EI-GCC, and by extension election officials across the country, prepare for, and manage, this emerging and evolving cyber risk. As with all communications plans, we recommend that this one be regularly updated by the EI-GCC, as the council further develops and defines its role.

More information is available on different types of communications materials for responding to a cyber incident. Election officials seeking examples of these additional materials can request the communications materials appendix to this document from NASS, NASED, or the EAC.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

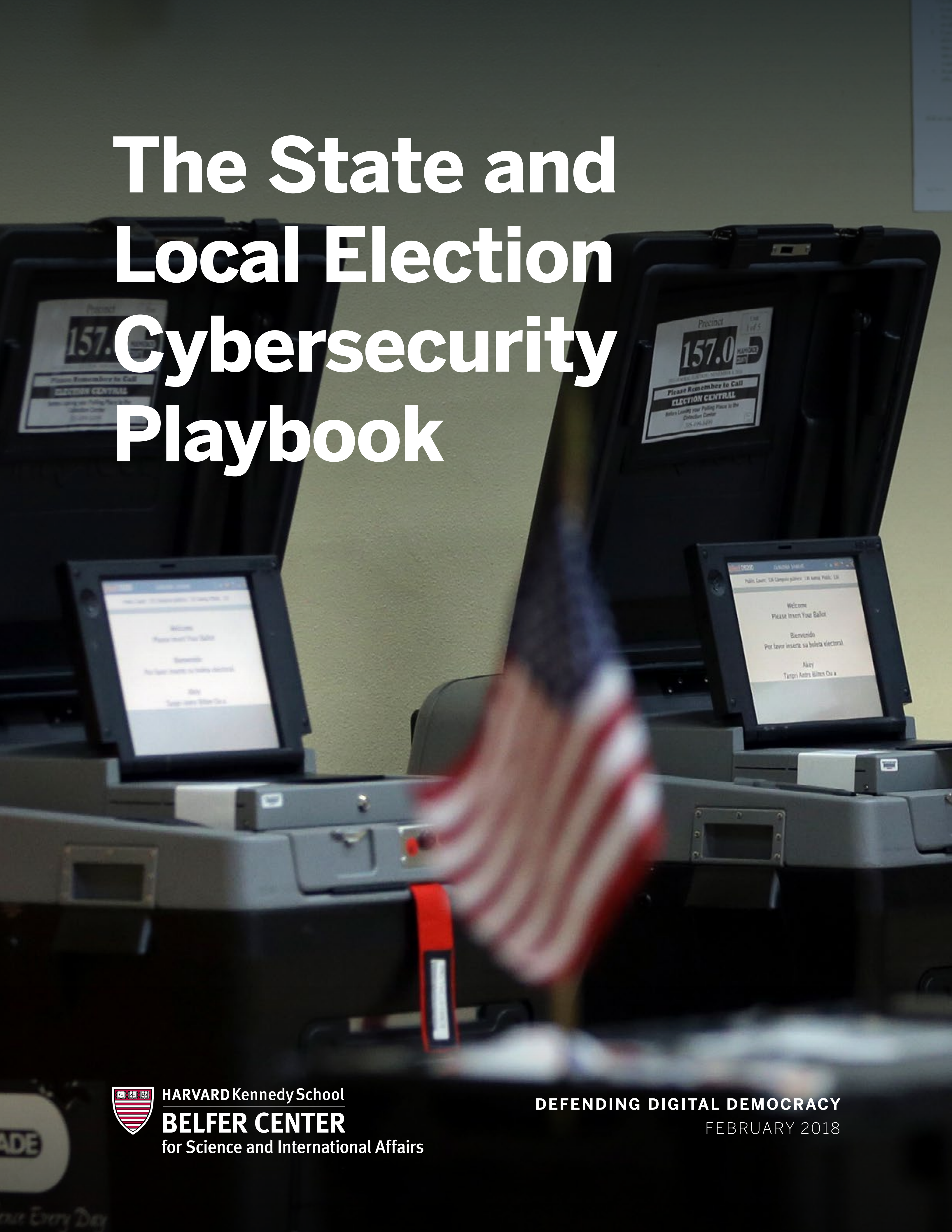
Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Harvard Kennedy School Belfer Center

The State and Local Election Cybersecurity Playbook

February 2018



The State and Local Election Cybersecurity Playbook

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Figure Illustrations by Jordan D'Amato

Cover photo: Voting machines in Miami Shores, Fla., Nov. 8, 2016, (AP Photo/Lynne Sladky)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

The State and Local Election Cybersecurity Playbook

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber attacks and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair. Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals. Now, in February 2018, we are releasing a set of three guides designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is The State and Local Election Cybersecurity Playbook.

D3P is a bipartisan team of cybersecurity, political, and policy experts from the public and private sectors. To better understand both the cybersecurity and other challenges that elections face, our team of nearly three dozen professionals spent six months researching state and local election processes. We visited with 34 state and local election offices, observed the November 2017 elections in three states, and interviewed leading academic experts, election equipment manufacturers, and representatives of federal government agencies. We conducted a nationwide security survey with 37 participating states and territories, which identified detailed nuances in election processes and their corresponding risk considerations. We hosted two state election cybersecurity conferences where we engaged state and local election officials in "tabletop exercise" election simulations to increase awareness of the cybersecurity threats they face and improve their ability to mitigate those threats.

This research taught us many things. Most importantly, we learned how difficult it is to defend the multifaceted nature of the elections process. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique. We were humbled by the intricacies of election operations in each state we visited, and inspired by election officials' incredible level of commitment to the democratic process. We also learned that the leadership of election officials is critical in creating a more secure system. Secretaries of state, election board members, state election directors, and local election administrators set the tone—it's ultimately their job to create a culture in which all staff make security a top priority.

This Playbook is intended for leaders at every level who play a role in running elections. While the future threats elections face are multifaceted, one principle stands clear: defending democracy depends on proactive leadership. This Playbook focuses on the U.S. experience, but it is also relevant to election officials around the world facing similar threats. We have designed it to identify risks and offer actionable solutions that will empower state and local election officials to protect democracy from those who seek to do it harm.

Finally, we would like to thank the election officials around the country for whom we wrote this guide. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

AUTHORS

Meredith Berger, D3P, Harvard Kennedy School

Charles Chretien, Software Engineer, Jigsaw (Alphabet)

Caitlin Conley, Executive Director, D3P

Jordan D'Amato, D3P, Harvard Kennedy School

Meredith Davis Tavera, D3P, Harvard Kennedy School

Corinna Fehst, D3P, Harvard Kennedy School

Josh Feinblum, Chief Security Officer, DigitalOcean

Kunal Kothari, D3P, Harvard Kennedy School

Alexander Krey, D3P, Harvard Kennedy School

Richard Kuzma, D3P, Harvard Kennedy School

Ryan Macias, Election Assistance Commission

Katherine Mansted, D3P, Harvard Kennedy School

Henry Miller, D3P, Brown University

Jennifer Nam, D3P, Harvard Kennedy School

Zara Perumal, D3P, Massachusetts Institute of Technology

Jonathan Pevarnek, Software Engineer, Jigsaw (Alphabet)

Anu Saha, D3P, Massachusetts Institute of Technology

Mike Specter, D3P, Massachusetts Institute of Technology

Sarah Starr, D3P, Harvard Kennedy School

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Arjun Bisen, D3P, Harvard Kennedy School

Drew Bagley, Sr. Privacy Counsel & Director of Global Cyber Policy, CrowdStrike

Daniel Bartlett, D3P, Harvard Kennedy School

Judd Choate, Colorado Election Director and President, National Association of State Election Directors

Amy Cohen, Exec. Director, National Association of State Election Directors

Mari Dugas, Project Coordinator, D3P

Alan Farley, Administrator, Rutherford County, Tenn. Election Commission

David Forscey, Policy Analyst, National Governors Association

Robert Giles, Director, New Jersey Division of Elections

Mike Gillen, D3P, Harvard Kennedy School

Chad Hansen, Senior Software Engineer, Jigsaw (Alphabet)

Eben Kaplan, Principal Consultant, CrowdStrike

Matt Masterson, Commissioner, Election Assistance Commission

Sean McCloskey, Election Task Force, Department of Homeland Security

Amber McReynolds, Director of Elections, City and County of Denver, Colo.

Joel Mehler, Senior Consultant, CrowdStrike

Robby Mook, Co-Director, D3P

Rachel Neasham, D3P, LoLa

Daniel Perumal, D3P

Debora Plunkett, former Director of Information Assurance, National Security Agency

Sean Quirk, D3P, Harvard Kennedy School

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

John Sarapata, Head of Engineering, Jigsaw (Alphabet)

Johanna Shelton, Director, Public Policy, Google LLC

Reed Southard, D3P, Harvard Kennedy School

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Charles Stewart III, Professor, MIT

Michelle K. Tassinari, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of Massachusetts

Frank White, Independent Communications Consultant

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

The Playbook Approach

Election officials are democracy's frontline defenders. Our election system faces an array of threats designed to undermine vote integrity and public trust in the election process. It is crucial that everyone involved in the election process—from top-level leaders, like Secretaries of State and Election Administrators, to day-to-day operators, like clerks and election site workers—understand their role in protecting the process and the threats that it faces. To this end, this Playbook has two goals: (1) to make the most likely and most serious cybersecurity and information operation threats understandable to everyone involved in the election process; and (2) to offer state and local election officials basic risk-mitigation strategies to counter these threats.

Our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals, but implementation of some strategies will require their involvement. We also did not address every issue or policy challenge that impedes cybersecurity readiness. Instead, we focused on the vulnerabilities and threats that align to create risk to our election process.

Finally, we understand that election officials already face many challenges in delivering accessible, accurate and secure elections—not least of which are constraints on financial and staffing resources. This Playbook is written with those realities in mind.

We hope this guide will give election officials more confidence in deciding how to approach security strategies and a greater common understanding in working with the technical specialists needed to implement these strategies.

This Playbook consists of three parts:

Background: frames the elections operating environment.

Common Ground: provides 10 best practice principles applicable to every election jurisdiction and a list of research security insights by election system.

Technical Recommendations: offers basic risk-mitigation recommendations specific to five components of the election system: voter registration databases, vote casting, vote tallying, election night reporting, and internal and public communications.

Our appendices offer more specific recommendations on two complex topics: vendor selection and maintenance, and election auditing. Additionally, the D3P Team has put together two additional resources to help navigate the challenges of maintaining and preserving public trust: "The Election Cyber Incident Communications Coordination Guide" and "The Election Cyber Incident Communications Plan Template for State and Local Election Officials."

Introduction

Running elections is complicated. It requires year-round preparation and coordination. Election officials have a lot to manage to ensure that the process remains free, fair, and accessible. Historically, efforts to protect the election system have focused on physical security, but today's digital world requires that we also focus on cybersecurity and information operations to defend against malicious actors of varying motives and means.

Cyber Attack: an attack targeting a network for the purpose of disrupting, disabling, destroying, or maliciously controlling it; or an attempt to destroy the integrity of data or steal controlled information. Common attacks include: spear phishing (to gain unauthorized access to existing accounts), denial of service (DoS), and device takeover.

Information Operations: the dissemination of information, true or false, to manipulate public opinion and/or influence behavior. Digital technologies like social media have made it possible for nation-states to organize information operations at an unprecedented scale. Because the tools needed for information operations are incredibly cheap and widely accessible (all you need is access to the Internet), adversaries use information operations to gain an asymmetric advantage over the U.S. and compete for influence in the world. Common information operation tactics include: spreading fake or misleading information online, leaking stolen information online, and using social media to amplify opposing views and stir political conflict.

Cyber attack and information operations tactics are often used in coordination. For example, a malicious actor might hack an election official's email account, alter emails, and then use those stolen, altered emails to spread misinformation online. Alternatively, social media login credentials might be stolen, and an official account then used to create confusion.

Background

What's at Stake

A core tenet of democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it wasn't in reality.

The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. While it didn't affect the outcome of the election, it did reveal significant vulnerabilities in our elections process. The 2016 case was not the first time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections, including the upcoming November 2018 midterm elections. While these foreign operations are traditionally a matter for the intelligence community and federal law enforcement, responsibility to secure elections ultimately falls on local and state officials.

Cybersecurity Threats to Elections

U.S. elections are decentralized. The federal government provides national-level guidance, but state and local governments administer elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters.

The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.

The "Who" Behind Cyber Attacks & Information Operations Targeting Elections

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.

POSSIBLE ACTORS

- Nation-State Actors
- Criminals
- Black Hat Hackers
- Insiders
- Terrorists
- Politically Motivated Groups

POSSIBLE MOTIVATIONS

- Financial Gain
- Retribution for Perceived Grievances
- Fame and Reputation
- Sow Social Division
- Foment Chaos / Anarchy
- Subvert Political Opposition
- Foreign Policy / National Interests
- Undermine Trust in Democracy

See the table on page 10 for an overview of known hostile actors.

KNOWN HOSTILE ACTORS THAT COULD TARGET U.S. ELECTIONS

Russia: The Department of Homeland Security, the U.S. intelligence community, CrowdStrike, and other private sector firms implicated Russian intelligence groups "Fancy Bear" and "Cozy Bear" in the 2016 U.S. presidential campaign hacks. Russian meddlers also probed information systems related to voter registration in 21 states, gaining access to at least two systems. Media sources also reported Russian hackers allegedly penetrated a U.S. election software vendor, hoping to gain information for a subsequent spear-phishing campaign against state and county election officials. In the run-up to (as well as since) the 2016 election, Russian-affiliated groups have conducted information operations using social media sites, exploiting existing fissures in American society. Similar coordinated efforts combining cyber attacks and information operations attempted to influence the 2014 Ukrainian and 2017 French elections.

China: In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials, or attempted to interfere with state election systems.

Iran: In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. If geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

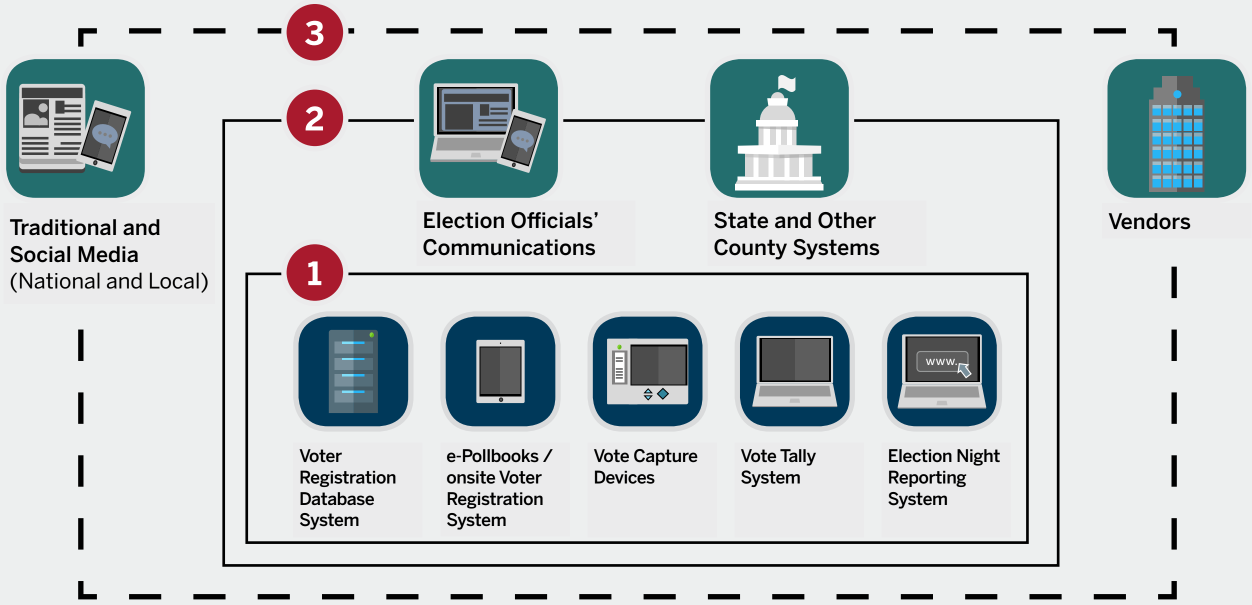
North Korea: While there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

The "How" Behind Cyber Attacks and Information Operations Targeting Elections

From a cyber perspective, every part of the election process that involves some type of electronic device or software is vulnerable to exploitation or disruption. When discussing election cybersecurity, the focus is often on voting machines. However, voting machines are only one part of a complex, interconnected system. Securing elections requires securing the entire process, because any element of the system could be the weak point that a malicious actor exploits.

We have broken the election system and its components into three levels of operation relating to cybersecurity risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level ❶ includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level ❷ includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. The third level ❸ involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.

ELECTION SYSTEM OVERVIEW: POTENTIAL ATTACK VECTORS


3
Traditional and Social Media (National and Local)
2
Election Officials' Communications
State and Other County Systems
Vendors
1
Voter Registration Database System
e-Pollbooks / onsite Voter Registration System
Vote Capture Devices
Vote Tally System
www.
Election Night Reporting System

Computers and software are present in every component of the election process, which means so are vulnerabilities. Depending on a malicious actor's motives, they could look to actually undermine the integrity of the vote, diminish public confidence in the process, or both. The potential attack vectors into an election system are both technical and human. They include those who develop and maintain the system, as well as the system itself. Ultimately, most cybersecurity breaches result from malicious actors exploiting human behavior, not technical shortcomings. This is true across all sectors and industries, and election systems will likely be no exception. Vendors of election systems or election software are also easy, valuable targets for malicious actors.

THE EXTENT OF VENDOR INVOLVEMENT IN ELECTIONS

Vendors play a critical role in supporting elections at both the state and local levels: from the computers used to access information, the servers that house information, the management of the databases that contain the information, the machines used to cast and tally votes, the websites and software used to display information and results, to the software that creates ballot designs or helps transfer information across systems. Some vendors are involved on such a broad scale that they can become a single point of failure at a national or state level. For example, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. In the 2012 presidential election, this vendor produced over 100 million ballots in more than 4,500 election jurisdictions and 40 states. The same single point of failure can exist at the state level. For example, one state contracted with a single vendor to do all of its state maintenance and ballot definition files for the 2018 elections.

The following figure describes common cyber and information operations that target each level of the election system. It provides a basic overview of the threats that election officials face from malicious actors.

Cyber and Information Operations

Some of the most common means and methods behind cyber and information operations used by malicious actors to target elections.

CYBER OPERATIONS

Social engineering is a category of attack in which malicious actors manipulate their target into performing a given action or divulging certain information (often a login or password).

Spear-phishing is a social engineering attack in which malicious actors send an email attachment or link that is designed to infect a device or obtain sensitive information. Malicious actors often review a target's social media accounts and work environment to tailor an email to appear enticing and convincing.

Hacking refers to attacks that exploit or manipulate a target system in order to disrupt or gain unauthorized access.

SQL injection is a way for attackers to read and/or alter the contents of a user's database by manipulating forms that are publicly available or exposed. Properly validating any incoming information from users can help prevent this method of attack.

Port scans are similar to checking whether doors are locked and walking through those that are open. Attackers often use it to profile potential targets and conduct surveillance on the systems they are running. A skilled attacker can use this method to gain access to unprotected servers or networks.

Man in the middle (MITM) attacks occur when attackers insert themselves between two or more parties and gain access to any information in transit between those parties.

Distributed Denial of service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access. Attackers disrupt service by using multiple computers and Internet connections to flood a target with excessive traffic, causing the service to crash.

Insider threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes.

INFORMATION OPERATIONS

Information Operations (IO) include propaganda, disinformation, and other tools used to manipulate public perception. Digital technologies have enabled adversaries to conduct IO at an unprecedented scale and to an unprecedented effect. In the context of elections, adversaries might use IO to undermine trust in an election result, exacerbate political divisions, or sow confusion and dissent.

Leaking stolen information: Attackers penetrate networks to obtain and leak sensitive information. Leaking information about budgets, election system vulnerabilities, or sensitive processes can reduce public trust.

Spreading false or misleading information: Attackers may hijack official accounts, or use social media or paid ads to distribute false information (e.g., polling times/places, election results), discredit a candidate, election officials, or voting system integrity.

Amplifying divisive content: Malicious actors often use existing social or political tensions to stoke divisions, distract, and disrupt a target to divert their resources.

Interrupting service to public-facing online resources: Attackers may use this tactic to accomplish a broader strategic objective. A DoS attack can serve to undermine trust in electoral systems or government services.

Common Ground

10 Best Practices that Apply to all Election Jurisdictions

Despite variations in election systems across states and localities, our 10 best practices can make any jurisdiction more secure. The list below provides overarching, high-level concepts. In the Technical Recommendations section, we operationalize these best practices into risk-mitigating recommendations addressing five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications.

1. **Create a proactive security culture**. Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared.

   Lead by example. Senior leadership, especially Secretaries of State, Election Administrators, and other heads of municipal jurisdictions, need to set an example for the rest of the organization. Issue guidance about the necessity of applying cybersecurity standards (such as those recommended in this Playbook), stressing the importance of cybersecurity for staff by personally introducing orientations and trainings, and following up with operations personnel on a regular basis about the implementation of improved cybersecurity protections. Leaders also need to ensure that those charged with implementing a cybersecurity program have the authority to enforce policies and procedures. Without enforcement, these are only words on paper.

   Develop a detailed cyber incident response plan. As with contingency plans for physical threats, teams should understand critical election system vulnerability points and create a detailed response plan (both internal processes and communications) for any system compromise. Leadership should also mandate frequent testing of critical systems to ensure both their resilience and officials' comfort with crisis management. Officials should extensively document any real or simulated incidents and review these periodically for training purposes.

   Use external resources to assist in improving cyber defense capabilities and building expertise. Department of Homeland Security and private sector technology companies are available to provide support for prevention and detection. Recognizing Constitutional and other legal restraints, National Guard cyber units, operating under state authorities, can also be a resource to help identify network vulnerabilities. These units are often made up of highly trained professionals involved in private sector cybersecurity.

Be diligent in selecting who is involved in election administration. Election systems qualify as national critical infrastructure, which raises the security expectations for those involved. Conduct background checks on all personnel involved in accessing sensitive information and privileged systems. Require vendors to do the same.

2. **Treat elections as an interconnected system**. Adversaries can target not only individual parts of the elections process but also the connections between them. Attackers look for seams: they seek the weakest point and move from there to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet—hacks can be executed using thumb drives and other external storage devices.

Safeguard computers and digital devices that touch the process, regardless of whether they are owned by a vendor, the state or local government, or are the personal device of an official or volunteer.

Centralize and streamline device security management by incorporating election offices into existing technology security plans.

3. **Have a paper vote record.** To protect against cyber attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data; every aspect from the ballot displayed to the voter to the recording and reporting of votes, is under control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or even to detect that an attack has occurred) after the fact.

Create an auditable paper record for every vote cast that is verified by the voter to ensure if the electronic vote count is maliciously altered, a true record still exists on paper. Make sure that this verifiable paper record has a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.*

> **Embed auditing** at points in the process where data integrity and accuracy are critical; for example, with voter registration records.

> **Make post-election audits standard practice**, using paper records to confirm electronic results.

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system.

> **Require strong passwords** not only for official accounts but also for key officials' private email and social media accounts. For your passwords, create `SomethingReallyLongLikeThisString`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of `$ymB01$`.

6. **Control and actively manage access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them.

> **Limit the number of people with access to the system** to those who need it to complete their jobs (the "who").

> **Restrict what each user is authorized to do** using the principle of "least privilege," meaning give users the minimum level of access that they require to perform their jobs (the "what"). For example, not every official from County A needs the ability to view or modify voter registration records in County B.

> **Quickly remove those who no longer need access**, regardless of their privilege level. Make this a part of standard offboarding procedures for staff.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems the most. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs.

> **Configure devices with sensitive data** to only be used for their specific purpose in the elections process (e.g., the software on a vote tallying computer is only what is necessary to run the election management system; or it operates on an isolated network so all wifi/bluetooth is disabled).

> **Restrict the use of removable media devices** (e.g., USB/thumb drives, compact discs) with these systems. A "one way, one use" policy is best.

8. **Monitor, log, and back up data.** Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross-county patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs.

> **Log any changes to the voter registration database**, and monitor the database with both a human check and anomaly detection software.

> **The adage is that "your data is only as good as your last backup."** This means that (1) backups should be regularly performed, either through automation or as part of a scheduled manual process, (2) backups should be read-only once created to prevent data corruption, and (3) backups should be regularly tested by performing a complete restore from backed-up data. Database technology vendors provide guidance and best practices specific to their technology and database architecture for validating and testing restoration of backups; consult these recommendations when developing your plan. In addition to those recommendations, ensure backups are stored in a different physical location than the master database and are physically secured.

9. **Require vendors to make security a priority.** In many states, vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. In our nationwide security survey, 97% of states and territories used a vendor in some capacity. Some vendors service multiple states— meaning an attack on one vendor could affect

many elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. (*For more details, see* **Appendix 1: Vendor Management***)*

Include explicit security stipulations in requests for proposals, acquisition, and maintenance contracts to ensure that vendors follow appropriate security standards, and guarantee state and local governments' ability to test systems and software.

Remember that skepticism is healthy. Verify security claims of vendors with independent analysis or reports from trained professionals.

Require vendors to provide notification of any system breach immediately after they become aware of it.

10. Build public trust and prepare for information operations.

Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. For additional information on communication strategies and planning see the D3P "Election Cyber Incident Communications Coordination Guide" and "Election Incident Communications Plan Template".

Communicate repeatedly with the public to reinforce the message that integrity is a top priority.

Before elections are held, start informing the public about cybersecurity threats, the steps taken to counter them (withhold specific details that could aid an attacker), and your readiness to respond in the event of an attack.

Establish processes and communications materials to respond confidently and competently in the event of an attack.

Build relationships with reporters, influencers, and key stakeholders to establish trust and have good communications channels before an incident occurs. It is especially important to do this with candidates and party officials.

Routinely monitor social media, email accounts, and official websites, and establish points of contact with social media firms (e.g., Facebook, Twitter) to enable quick recovery of hacked accounts.

Security Insights by Election System

During our field research we learned a lot of great insights from election officials who are making cybersecurity a reality. This list reflects many of those ground-level insights, classified by the key components of the election system. For detailed technical specifications, refer to the Technical Recommendations section.

VRDB

- Patch and update all computers and servers that connect to the database.
- Ensure the database server is not accessible over the public Internet. Restrict which external systems can write directly to the database.
- Establish a baseline for normal data activity (new entries and edits to existing entries). Monitor activity against this baseline and investigate anomalies. Add human review for data changes—at a minimum, review weekly change summaries; ideally have an official review automated updates.
- Limit access to only those who need it. For those with access, restrict access to only their area of responsibility (e.g., a county official can only edit files for his/her county but may have read access to others). Regularly adjust access and permissions as personnel change.
- Require two-factor authentication for anyone to log into the database—no exceptions.
- Make frequent backups of the VRDB. Conduct routine recovery drills to ensure they work.

For Online Voter Registration

- Do NOT allow web servers to connect directly to the VRDB.
- Have mechanisms in place to mitigate DDoS attacks on the voter registration website.

For e-Pollbooks

- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Make them single-purpose devices; software on them should only be what is necessary.
- Understand how voter information is loaded onto the e-Pollbooks; cryptographically confirm the e-Pollbook file on the device matches the original file.
- Physically disable or otherwise seal exposed ports if possible.

Vote Casting Devices

- Every machine should have an individual voter-verified paper trail.
- Do election audits. Make them a regular part of the elections process.
- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Do not connect machines to any network for longer than necessary (i.e., if wifi is used to update, ensure it is enabled only for the required time window).

- If vote tallies are transmitted directly from the machine, ensure the data transmission is encrypted.
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy:" only use physical media once, from one system to a second system, then securely dispose of it.
- Ballot definition files could be corrupted—secure the creation, transfer, and upload process.

Vote Tallying Systems

- Vote tallying systems should be single-purpose systems, with only software installed required for running the vote tallying system—nothing else, and isolated with no network or Internet connectivity.
- Electronic vote tabulation data should be encrypted when transmitted between sites.
- Address security vulnerabilities by patching and updating vote tallying system devices.
- Use two different forms of communication to report and confirm vote tally reports (e.g., electronic file submission, then phone call).
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy." Only use physical media once, from one system to a second system, then securely dispose of it.

Election Night Reporting

- Ensure websites are up to date and create a plan for DDoS mitigation.
- Limit access/edit privileges for users, similar to VRDB access.
- Prepare a contingency communications plan for disseminating results.
- Verify that results shown to the public on the official ENR website match reported results.
- Monitor the ENR system for anomalies in traffic or access during election night.
- Conduct searches/media reviews during election night to check for false sites and social media accounts.

Internal and public-facing communications

- *Email:* Use two-factor authentication for email accounts.
- *Public-facing websites beyond ENR (e.g., to communicate election day logistics):* Keep sites up to date to decrease potential for manipulation; have an action plan for potential DoS; know how to recover hijacked accounts.
- *Official social media accounts:* Use two-factor authentication. Limit access. Understand third-party apps can be a vulnerability if they are compromised. Identify points of contact and establish relationships with key social media firms for responding to issues when they arise. Know how to recover hijacked accounts.
- *Private social media accounts*: Private accounts of key officials need to be secured as they are also likely targets.

Vendors

- Require vendor security measures. Vendors can connect to every part of this system. Their internal security matters—vendor access points could be the weak link that gets exploited and corrupts other parts of the process.
- Ensure security requirements and considerations are included in vendor contracting and enforced.

Technical Recommendations

Securing State Election Systems

There is no such thing as perfect security; however, there are preventative measures that make the process much more secure. In the Common Ground section, we provided best practices that apply across all election jurisdictions and some system-specific insights. In this section, we elaborate on these concepts with specific technical recommendations as they relate to five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications. As we highlighted in Common Ground, system defense is a critical first step in securing the elections process. For this reason, the majority of our recommendations fall into the category of "Protect." Because election systems are decentralized and varied in nature, not all recommendations apply to every state or locality.

As we said in the introduction, our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals. But we do want to emphasize IT professionals are critical to establishing and maintaining a secure election system and their expertise will be needed for many of our recommendations. Threats are constantly evolving and IT professionals will help you get beyond what this Playbook provides and keep you abreast of the latest threats and defenses.

Voter Registration Databases and e-Pollbooks

Voter registration databases (VRDBs) store information on registered voters in a given state. The Help America Vote Act requires that all states implement a "single, uniform, official, centralized, interactive, computerized voter registration list," unless the state has no voter registration requirement. Throughout this document, we refer to this centralized, computerized list as the VRDB.

Different states follow different processes for managing and updating their VRDB—in some states, all new entries, deletions, and edits are implemented as processes at the state level, whereas in other states this happens at the county level (with changes pushed up to the state-held "master"). In many states, ***third-party systems***, such as Health and Human Services and the Department of Motor Vehicles, provide data to the VRDB in an effort to keep voter records up to date. Some states offer ***online registration***, allowing voters to register and edit their record via a public-facing online portal connected to the VRDB. Some states offer ***same-day registration***, while others require voters to register before election day.

Closely linked to VRDBs are the pollbooks used on election day. States may choose to only use paper pollbooks, or may use ***electronic pollbooks (e-Pollbooks)*** to process voters on election day. e-Pollbooks are electronic versions of voter rolls used by polling site officials to verify legal voter registration and related details on election day. These are usually tablets or laptops and can be networked into a central voter registration system (allowing them to check and update voter records in real time, for example to allow for same-day voter registration), or they can be standalone at the precinct (containing a separate, offline copy of the electors list). Regardless of whether a state/county uses paper or e-Pollbooks, their creation requires an export of files from the VRDB for either printing or translation into an e-Pollbook compatible file.

Across both VRDBs and e-Pollbooks, states may choose to develop and maintain the software in-house, or may outsource this work to an external ***vendor***.

Core VRDB issues

KEY THREATS:

Unauthorized access to the VRDB from Internet exposure: Leaving the VRDB exposed to the Internet makes it vulnerable to attacks. Once it is connected to the database, an attacker can add, edit, or delete voters, allowing for false votes to be cast on election day or forcing voters to cast provisional ballots. Even if this does not affect actual vote outcomes, the perception of vote manipulation or voter suppression can significantly undermine the credibility of an election.

Maintenance: An insufficient or poorly timed maintenance and patching regime leaves security vulnerabilities open and can expose the VRDB to attacks.

Account compromise: Attackers might compromise the accounts of election officials with access to the VRDB; without proper controls in place this could allow the attacker to add, edit, or delete voter entries. In the absence of proper logging and monitoring, these changes may go unnoticed until election day and affect the ability of voters to cast ballots.

Third-party system compromise: Third-party systems (e.g., DMV, HHS) linking into the VRDB can be compromised, or the transmission of these entries to the database could be compromised along the way. If these systems are allowed to feed directly into the VRDB, or if the review and approval process at the state and county level is insufficient, there is a risk that the compromise could allow malicious actors to manipulate voter status.

Recommended actions:

Identify

Map how other systems connect to the VRDB. They will commonly be connected to sync or add voter information (e.g., from DMV records).

Know where the VRDB is hosted and what defenses exist on the servers and the underlying network infrastructure.

Know what accounts have access and what level of access each account has (e.g., can a county official change records from other counties?). Use a test account to verify that restrictions are operating as intended.

Determine which of the servers can be accessed over the Internet. Close connections to any that do not require access.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can edit the VRDB. Account security is crucial for all VRDB users and especially those with elevated or administrative privileges.

Conduct penetration tests, source code audits, and encourage vulnerability discovery efforts. Regardless of whether your VRDB software is built in-house or by vendors, third-party auditing and penetration testing should be performed to provide awareness of security vulnerabilities. Develop and maintain a continuous program that tests your organization's susceptibility to spear phishing and other social engineering attempts. It is important to do this regularly, both to spot new vulnerabilities that might arise, and to prevent staff from becoming complacent.

Apply software updates and patches. Applying software updates and patches on all devices connecting to the VRDB is essential to preventing malicious actors from gaining access. Check for patch signatures to ensure they are authentic. Using endpoint management software and vulnerability software on official computers can help automate the patching process to ensure systems stay up to date.

> To prevent interference with election day operations, **establish cut-off days for applying and testing patches** to ensure optimal functionality during election periods. Only critical updates should be done after the cut-off window and all patches should be tested for functionality as well as security.
>
> **Create automated scans** to look for vulnerabilities on the VRDB portal.

Ensure that your underlying database server is not accessible over the Internet.

Restrict external systems' access to the VRDB. Data from other systems (e.g., the DMV) should go through validation (either manual or automated) rather than allowing those systems to directly write to the database. This prevents the database from being directly edited if an external system is compromised.

Log changes. As a rule, changes to the VRDB should be recorded securely and be reviewed, preferably both by a human and an automated system. Establish a baseline for normal data activity (e.g., new entries, edits to existing entries, change in voter status) so that atypical behavior can trigger an alert.

Limit account access to the VRDB. Restrict access to the database to those who need it and diligently maintain and review this access list. For example, state or local offices responsible for updating voter registration information require access. However, the software developers who designed the system do not. Account management includes revoking the access of old employee accounts immediately after they depart or change roles. Vendors responsible for the software will need access, but should not retain that access any longer than necessary.

Implementing these limitations requires an individual to be responsible for constantly managing accounts, ensuring existing accounts belong only to those who need them, and that system permission changes were approved.

Permissions Management for VRDB accounts. Everyone who has an account should be given specific permissions that dictate what they can and cannot do. More people with more access means an increase in potential avenues of attack on the VRDB, so limit the degree of access for each account to only what is necessary for that employee to do their job.

> The most common levels of permission variation are "read," "write," and "admin" access. Someone with "read" access can only read the data, but not alter it; someone with "write" access can change data; and someone with "admin" access can alter permissions for other users.
>
> Even within those levels of permissions the scope of access should be tailored. For example, a county administrator may need access to their own county's information, but should not be able to access information from another county.
>
> **Consider implementing permission restrictions** that limit the number of changes one user can make during a certain time window to stay in line with normal activity patterns—this helps guard against both insider threats and account compromise.

Require users to access the VRDB portal using a VPN. This ensures that even if an account is compromised, the attacker is unable to use it without VPN credentials.

> **Whitelisting** can also be used to limit either what devices a user can connect from or which locations. Paired with a device inventory database, requiring device certificates will allow you to restrict access to managed devices that are verified as secure. Another option is IP whitelisting, which can restrict access to users at specific location. This would require coordination with remote offices' IT departments to identify what addresses should be whitelisted. Using IP whitelists would force an attacker to compromise a machine at one of the locations before they were able to begin an attack against the VRDB.
>
> Establish policy that does not allow connections to the VRDB from public, unauthorized, or unknown devices.

Detect

Monitor activity against a baseline and investigate anomalies. This allows you to notice unusual trends that deviate from the norm. At a minimum, this should be a technical (automated) check which occurs at both the state and county level. Automated monitoring of anomalies at the state level is critical to detect broad changes across the state that may not be noticeable when monitoring only at the individual county level.

Incorporate a human review into data change monitoring to augment technical monitoring. Experienced election officials providing human monitoring at the local level may reveal subtle manipulations. Election officials should trust their instincts—they are more familiar with this data than anyone else. Empower these officials to flag suspicious behavior or anomalies and investigate them. While human review of every record change is not realistic for all localities, weekly change summaries should be required at a minimum.

Monitor permission changes: Make sure that when changes are made, they are reviewable by those with similar access levels. Create the framework for conducting regular reviews of those changes. This process will allow unusual activity to be detected sooner.

Mail confirmation of changes in registration to voters (ideally both to their old and new address).

Respond

If the incident involved an attacker gaining access to VRDB, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If a physical machine was compromised, disconnect the machine from the network and seek professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Execute the recovery plan during an incident or after one occurs. Include the following categories in your plan: Recovery planning, improvements, and communications.

Public communications around a voter registration-related incident is a CRITICALLY IMPORTANT issue when it comes to public trust and elections transparency. It must be deliberately executed with tremendous care. See D3P's *Elections Cyber Incident Communications Plan Template*.

Practice restoring from VRDB backups. If there is a second live VRDB system, be sure to practice using the secondary system.

Lessons learned should be shared and incorporated into the existing recovery plan. Where possible, update your system to prevent a similar failure or exploit from occuring again in the future.

Vendor Considerations

The most common forms of vendor support for voter registration databases are:

- Vendors building and maintaining the VRDB
- Vendor building and state or county maintaining of the VRDB (to include modifications to initial vendor build)
- Vendor and state jointly building and maintaining
- Third party vendor used to assist with maintenance

The General Vendor Recommendations 1-8 at the bottom of the Technical Recommendations section provide best practices for working with vendors and mitigating potential cyber vulnerabilities. The type of vendor involvement and timeframe (set time period involvement versus continuous) will impact how they apply for each state/county. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Online Voter Registration

States that offer online registration are exposed to the following additional threats:

KEY THREATS:

Website spoofing: Attackers could pose as the official website to either give voters the illusion that their information is updated or in an attempt to capture that information.

Distributed Denial of Service: Attackers can conduct DDoS attacks on the public-facing voter registration website, preventing voters from registering and potentially discouraging them from participation.

External connectivity: An unsecured website presents another vector for a malicious actor to penetrate the VRDB. If it is not properly secured, an attacker may be able to use it to change any vote record.

Large-scale data alteration: An attacker could use information leaked on the Internet to impersonate many different voters and attempt to update their registration details.

Recommended actions:

Identify

- Know who the domain name registrar and web hosting provider are and how to contact them.
- Determine who is responsible for keeping the website software up-to-date.
- Know who has the ability to edit the website.

Protect

- Do NOT allow web servers to connect directly to the VRDB. This restriction significantly reduces the possibility of a website vulnerability leading to a compromise of voter records.
- Require a CAPTCHA to change a voter's registration. This is a short task, ranging from clicking a checkbox to typing the characters shown in an image, which verifies that an online form is being submitted by a human and not a machine. It increases the difficulty of a computer program changing hundreds or thousands of voter registrations at once.
- Protect the online voter registration website against DDoS attacks.
- See the **Website** section for additional details on securing the public-facing component.

e-Pollbooks

KEY THREATS:

e-Pollbook Data Manipulation: A malicious actor is able to gain access to the device either using a wireless connection or because the physical device was not properly secured. Once on the device they are able to manipulate the voting roll—either deleting or altering existing voter registration data.

Altering of State Voter Roll via e-Pollbook: If an e-Pollbook has a live connection to the state election day voter roll, compromising one device could be used to change statewide records.

Maintenance/patching of e-Pollbooks: The difficulty in which an e-Pollbook device is compromised depends heavily on whether it is updated and patched. Failure to do so will provide malicious actors an opening into the device.

Recommended actions:

Identify

Examine all the possible functionalities of the device and identify the components you intend to use. Specifically pay attention to the wireless and networking functionality.

Know what kind of network connections your e-Pollbooks need.

Understand how voter information is loaded onto the e-Pollbooks.

Protect

E-Pollbooks should be single-purpose devices. Software on the device should be limited to what is necessary for their use.

Verify the integrity of the e-Pollbook file.

> Cross-check the data on the pollbook with what is in the VRDB.
>
> Use digital signatures and hashes to verify the integrity of data contained in voter roll files that are transferred between systems and to ensure data has not been maliciously altered or compromised. If using a method that requires data transmission over a cellular network or the public Internet, use a virtual private network (VPN) to secure those transmissions.

VERIFYING FILE INTEGRITY USING HASHES AND DIGITAL SIGNATURES

A hash is like a fingerprint for digital files—the *hash* of a file will not change unless the actual file changes. Using a hash while transferring files will allow you to confirm that the file has not been altered in transit if the hashes computed by each party are the same. If you decide to use a hash, transfer it through a different channel than you used to obtain the files and compare it to the hash you compute. By sending them separately, such as downloading the file from a website and reading out the hash over the phone, you prevent the attacker from changing the hash at the same time as the file.

A more secure option is to use a digital signature. It is a form of encryption which is equivalent to a seal on a physical document; it guarantees that the file came from a specific trusted source and that its contents have not been modified in transit.

- **Ensure all devices are updated and patched.** Test the e-Pollbook to ensure that it is fully functional after patches have been applied.
- If you do not need the e-Pollbook to be connected to a vendor, VRDB, or the Internet while voting is taking place: **turn off bluetooth and wireless capabilities on the devices.** It is better to disable these functions at the hardware level (e.g., removing the wireless card) than to change a setting whenever possible.
- If you need to connect to external systems:
  - **Connect over a VPN** or other encrypted channel.
  - **Ensure that the entire setup is preconfigured** and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
  - **Do not connect e-Pollbooks directly to the VRDB.** Set up a separate system (essentially a copy of the VRDB) to handle changes to voter information, which prevents the VRDB from being impacted if an e-Pollbook is compromised.
  - **Restrict edit access only to juridictions that need it.** If state law requires you to vote in precinct and there is not same-day registration, an e-Pollbook in one precinct should not be able to modify the voter's record from another precinct.
- **Have a paper backup** of the e-Pollbook.
- **Ensure physical security.** Cover exposed ports (e.g., USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. Do not use anything other than the charging cords provided with the e-Pollbook on receipt (e.g., do not use an iPhone charger or other similar charger that is not actually part of the e-Pollbook election day pack).

Detect

Monitor data changes. Counties or vendors, as applicable, should monitor voter roll files for anomalies in changes or access. Implement data controls around normal data activity that prevent large-scale changes.

Perform vulnerability scans of e-Pollbook devices to identify those that do not have the latest security updates. Apply patches to minimize vulnerabilities.

Respond

If the incident involved an attacker gaining access to a networked voter roll file shared beyond a single polling site, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If the e-Pollbook device was compromised, disconnect the machine from the network and seek out professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Have a backup paper copy of the pollbook on site and backup devices pre-programmed for deployment to sites, if necessary.

Vendor Considerations

The most common forms of vendor support for e-Pollbooks are:

- Building and/or maintaining of e-Pollbook devices and software.
    - Can overlap with vendor support for VRDBs.
    - Can involve live monitoring of e-Pollbook operations on election day.
- Building electronic voter roll files for e-Pollbooks based on VRDB info where a compromise of the vendor could result in voters being missing, or incorrectly added to, the roll.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Vote Casting Devices

Overview: Vote casting devices serve as the primary conduit for the actual ballot marking or mark recording process on election day. Most states and counties today use some variation on two types of vote casting devices:

> **Optical Scanner (OS) or Digital Image Scanner:** A machine that scans (and often digitally records an image of) marked paper ballots. Voters cast a ballot via traditional pen and paper, an electronic ballot marking device, or some alternative marking method. The marked paper ballots are then run through these scanning machines which records the appropriately marked vote for each race, and then calculates running vote totals for all ballots scanned on the machine. The machine prints a total result after polls close. The initial paper ballot ensures that a physical record exists for audit or other vote verification purposes.

> **Direct Recording Electronic (DRE):** A DRE system presents a digital ballot image to a voter, collects the voter's selections, and records those choices directly onto electronic media. DREs may be fitted with voter-verified paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction.

In recent years, alternate voting methods, particularly vote-by-mail and early voting, are becoming increasingly popular with voters. These jurisdictions often utilize central count facilities where paper ballots are consolidated for tallying. At central count facilities larger variations of the optical scanner/digital image scanner are often used for paper ballot counting.

KEY THREATS:

Device tampering: Voting machines can be compromised via physical tampering (including using removable media) or through external connectivity (e.g., WiFi). This would allow the attacker to change the reported vote information.

Inability to detect tampering: Some DRE machines do not produce a VVPAT (because optical scanner systems scan paper ballots, they do not face this threat). Should a malicious actor compromise such a machine, votes could be lost and results thrown into question.

Recommended actions:

Identify

Examine all the possible functionalities of the device and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.

Know the certification status of all your equipment. The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

Protect

If you have a DRE machine that does not produce a paper trail, **you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**

Physical Security/Access Seals. Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.

Penetration test systems. Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote casting devices.

Restrict device functionality to what is required. Even if you have disabled a feature through a settings page (such as wifi connectivity), those features could still be exploited. You should not trust that toggling a switch in software will actually disable the functionality. If possible, the hardware should be removed.

Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem. If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.

> **Create a copy of the results** (either a printout or by saving it to removable media) before you connect to the network.

If removable media is used to transfer data (e.g., ballot definition files, vote tallies):

> **Have a procurement strategy for devices.** Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.
>
> **Protect device chain of custody.** Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical

record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.

One-way/one-time use: Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.

Scan media devices for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

Detect

Perform logic and accuracy testing of the programmed device.

Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

Respond and Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Handling ballot definition files and other software updates

KEY THREATS

Supply chain interdiction: A malicious actor could use vendors as a pathway to plant malware to modify or compromise a ballot definition file before it reaches the hands of election officials.

Manipulation of ballot definition files: If an attacker obtains access to the original ballot definition file, this could leave machines susceptible to destructive attacks and/or could affect tallies.

Recommended actions:

Identify

Determine who is responsible for, and what machines are being used, to create the ballot definition file.

Determine how the ballot definition file is being transmitted to the vote casting device.

Protect

Treat the ballot definition file as critical information. As such, limit its exposure to compromise as much as possible. The system used to develop the file should be isolated from external network connectivity. Place a tamper-evident seal over the media containing the ballot definition file.

Conduct testing (e.g., logic and accuracy, parallel testing) on the systems that the ballot definition files have been loaded onto before deploying them for use.

Review ballot definition file source code to prevent malicious code distribution. When possible, review source code before final distribution of ballot definition files to avoid dissemination of malicious code.

Secure the creation mechanism of the ballot definition file: The ballot files should be generated on a secure single-purpose and air-gapped machine

Secure the transmission of the file:

> If possible, use digital signatures on the file. Forcing the voting machines to verify the file signature before loading it will prevent attempts to change the ballot files after it has been created.

- If using removable devices to transfer the files, follow all best practices, including one-way and one-time use. The section on vote casting devices above discusses more specific recommendations for removable media.

Detect

- Verify the seals over media containing the ballot definition file.

- Scan ballot definition files for malware. If you detect abnormalities, don't use the files and contact forensic experts for assistance.

Recover

- Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

- Vendors often interact with ballot files by:
  - Creating the files themselves
  - Transferring the ballot files to the voting machines

- See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Vote Tallying System

Vote tallying covers the various devices and networks used to tabulate ballots and aggregate results. Based on differences in setup across states and counties, this process can start at the polling site (for example, precinct count optical scanners that tabulate ballots onsite), or at more centralized counting facilities. In many instances vote tallying is conducted at the county level, where voting sites through a variety of methods (e.g., phone call, email, thumb drive/USB) provide counties with their respective vote tally totals. This section discusses common threats and remedies seen across many system set-ups.

KEY THREATS:

Manipulation of tabulation systems: A compromised tallying machine at a polling site or central counting facility could allow an attacker to directly manipulate tallies before they are transmitted to the county or state.

Data transmission with removable media: USB devices—and other portable physical media—are often used to transmit results from precincts or centralized counting facilities to segmented county/state networks. USB devices can be exposed to malware and compromised at the supplier level or through a previous use in an infected machine. This compromise could result in manipulated data and could also lead the tallying machine itself to become compromised, exposing the system to future exploits.

Networked data transmission: In tallying setups where votes are tabulated at the polling station and transmitted to the county, or are transmitted from the county to the state through a system other than the election night reporting system, configuration errors in the modem, wifi, or cellular network connections used for transmission can leave the process vulnerable to "man-in-the-middle" attacks. These allow adversaries to manipulate results before they are received at the county (or state) level.

Denial of service: Counties or, where relevant, states, receive results from precinct or centralized counting facilities over the network. Servers can be targeted with a DoS attack by an adversary, resulting in delays in vote reporting during election night.

Recommended actions:

Identify

Know the certification status of all your equipment. The EAC's Voluntary Voting System Guidelines (VVSG) provide federal level certification standards. Many states have their own certification process.

Protect

Vote tallying systems should be isolated from any networks or overall Internet connectivity (commonly referred to as "air-gapped"). This includes connecting to voting machine modems. In the case where you cannot achieve total isolation, restrict network access to precincts and counties to prevent outsiders from accessing or slowing down the system. Again, the best practice is to keep these machines totally isolated and to transfer results to them using removable media as they arrive. As for all removable media, practice the "one-way, one-use" rule.

Use a dedicated single-use system for vote tallying. Using a system solely for vote tallying and disabling unnecessary functionality, like network connection, can limit exposure to attackers.

Require strong passwords and implement two-factor authentication to access the vote tally system device. There are two-factor authentication methods that do not require network connectivity, and that can be implemented.

Use a digital signature to verify the source of vote tallies. Requiring each voting machine to digitally sign its report will prevent a malicious actor from introducing fake results into the tally process.

Keep devices up to date and fully patched. Despite the tally system being air-gapped, it is still important to keep the software on them updated. Review available updates, test how they work with your system, and apply them. You should establish a cut-off date prior to the election after which you will not change the software in order to provide enough time to test the system.

System testing. Include the tallying system in your tests of the system. While conducting penetration tests, teams should look for ways they could access these machines despite the air gap (including testing the physical security) and other ways to force errors in the tallying process.

Detect

Report vote tally totals using multiple forms of communication (redundant communication). For example, electronic vote tally submissions should be confirmed with a follow-up call or text.

Recover

If the electronic system is compromised, implement hand-count procedures.

Vendor Considerations

In many cases, the machines used to tally results will have been provided by vendors who will be involved in the maintenance of those machines. A compromise at this level could cause vote totals to be calculated incorrectly, compromising public trust in the election even if the correct totals are eventually reported.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Election Night Reporting (ENR)

Election night reporting (ENR) consists of the systems and processes for aggregating and communicating the unofficial election results to the public and media after polls close, usually via a website. Counties and states may also report election night results via social media—please see the Internal and Public-facing Communications section for best practice in securing social media accounts. ENR setups vary by state across three principal dimensions defined below:

> **How ENR relates to the vote tallying process**. ENR can be closely linked to the vote tallying process (e.g., a state's non-public vote tallying system might automatically submit results to the state's public ENR website), or can be run separately and in addition to the tallying process.

> **Whether ENR is run by the state, counties, or a combination of both.** Most states run ENR centrally, with counties (or in some cases municipalities) submitting results to the state via a centralized ENR system. In some of these cases, the counties run separate, additional ENR systems (e.g., to provide further granularity on results). In a small number of states, ENR is managed at the county (or municipality) level.

> **Who builds/maintains the ENR system**. Regardless of whether ENR is run at the state or county level, ENR systems can be developed and managed in-house (by the state or county), developed by a vendor but managed in-house, or developed and run by a vendor.

KEY THREATS:

Transmission: In a state-run ENR setup, counties submit their vote reports to the centralized system provided by the state. A configuration error could make this transmission vulnerable to "man-in-the-middle" attacks, where adversaries manipulate vote reports before they are received by the state.

Manipulation of ENR systems: Configuration errors can leave ENR systems vulnerable to exploits or unauthorized access, allowing adversaries to manipulate the vote counts after they have been received in the (state or county) ENR system.

Denial of service: In a state-run ENR set-up, a DoS attack on the transmission of ENR results can lead to a lack of results being reported for one or more counties. In addition, attackers can conduct DoS attacks on the public-facing ENR website, making result reporting unavailable to the public/media altogether during election night.

KEY THREATS (CONTINUED)

Website spoofing: Attackers could redirect public inquiries to a spoofed website, which pretends to be the official ENR system but in reality is controlled by a malicious actor. For example, this could be used in disinformation campaigns to depress voter turnout by saying an election has already been called.

Recommended actions:

Our recommendations should be implemented by the county, state, or external vendor, as appropriate.

Identify

Identify which offices need access to the ENR site or other medium through which they report and consolidate results.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can access the ENR system.

Secure transmission channels. Require users to authenticate themselves when adding result information and restrict the results they are able to change to only what is within their purview. Ensure all network traffic is secure (e.g., enable SSL on a web-based portal).

Limit access through restricting write privileges for users across the state and counties or within the county as applicable. In state-led ENR systems, specifically ensure that each county can only edit its own vote reports (not those of other counties).

Log incoming election results to help trace and correct inaccurate reports.

Prepare a contingency communications plan for disseminating results if the primary medium is unavailable.

Publicly communicate about ENR process to preempt spoofing. Communicate clearly, ahead of any election, how the state or county will report vote results during election night, to preempt false ENR websites from popping up.

Protect ENR websites against DoS attacks. See Website section for additional recommendations.

Report election night results using multiple forms of communication. They should be confirmed over a second channel; for example, a follow-up call, on top of being sent through the primary channel.

Detect

> **Each county/precinct should verify that results shown to the public on the official ENR website match the results they reported.**

> **Monitor the ENR system for anomalies in traffic or access during election night.** Especially monitor any attempts to change the displayed results (e.g., failed login attempts to the portal) or traffic that may be part of a DoS attack.

Respond and Recover

> Public communications around election night reporting are critical. Have a backup plan for how to publicize either that your reporting website is showing no results, or incorrect results. Include the specifics in your communications incident response plan.

Vendor Considerations

> Vendors are often responsible for building and/or running both the system for updating results and the webpage that displays those results to the public.

>> Be sure that you have an internal (state and local level) backup plan for how to publish results if the vendor system is unavailable.

> See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Internal and Public-facing Communications

Running successful elections requires extensive communication—both within state/county election teams, and with the public. This tends to consist of four key communication channels: internal email communication, official election-related websites, official social media accounts, and the private social media accounts of key officials. All of these communication channels could come under attack by adversaries who abuse them to cause confusion about election logistics before or during election day, and/or to undermine the credibility of the election overall.

INTERNAL COMMUNICATION

Email communication ahead of and during the election is crucial for the election team to coordinate activity internally among states, counties, and precincts/polling stations.

KEY THREATS:

Account compromise: Attackers could compromise key officials' email accounts to send out false information to members of the election team—for example, asking for polling stations to close early or for polling stations to switch to paper pollbooks due to an alleged issue with e-Pollbooks (resulting in delays and lines forming). In addition, compromised accounts could be used to distribute malware across the election team's devices. Clearly, access to the email account of any member of the election team—even at a low level in the organization—exponentially increases the chances of subsequent attacks on the email accounts of more senior members of the election team succeeding.

Recommended action:

Implement two-factor authentication for all official accounts. In most cases, adding a second factor will be enough to prevent an attacker from compromising an account. In addition to this, require strong passwords.

Require all messages to come from official accounts. While officials should take steps to secure their personal accounts as well, all official communication should be done through accounts that have been carefully secured by your IT department.

PUBLIC-FACING COMMUNICATION

Election officials communicate extensively with the public through both ***official election websites*** and ***official social media accounts*** (e.g., Election Board's Twitter account, Secretary of State's official Facebook account). This communication is separate from, and in addition to, election night reporting (which we cover in the section above), and includes, for example, communication to raise awareness of upcoming elections, key deadlines, (e.g., for online registration) and election day logistics (e.g., poll locations, opening hours, ID requirements).

While not officially part of a state's or county's public-facing communication, the ***private social media accounts of key officials*** (e.g., the Secretary of State's private Facebook account) could be used to communicate false election-related information to the public. These should be protected with the same care as the organization's public accounts.

Official Websites

KEY THREATS

Website manipulation (e.g., changing information on polling place location): Malicious actors could look to sow confusion or discourage voters by manipulating the information on official websites. For example, attackers could alter polling site locations and times to make it harder for voters to find their designated vote site

Spoofed websites: To sow distrust in the process, attackers may replicate the official state or county website and post the opposite results than is being reported—for instance the winner of Race A is now the loser.

Distributed denial of service attacks: Similar to voter registration sites, attackers could attempt to shut down official websites on election day to inhibit voters from knowing their designated voting location.

Recommended actions:

Identify

Know who your web hosting provider is and how to contact them.

Determine who is responsible for keeping website software up-to-date.

Know who has the ability to edit your website.

Protect

Have automated procedures to keep software (e.g., Wordpress, Apache) up-to-date. Website software needs to be updated on a regular basis in order to patch vulnerabilities as they are discovered. Have a system for tracking what version of software you are using and what vulnerabilities are discovered and ensure that those vulnerabilities are patched.

Conduct penetration testing and security audits for all resources. Regardless of whether your website was developed by your staff or by vendors, a third-party audit and penetration test can identify vulnerabilities. This should be done anytime a major change is made to website software.

Ensure that developers have been trained on what the common attack vectors are. One good guide for these is the Open Web Application Security Practice (OWASP) Top-10 list.

Ensure sufficient capacity to receive increased site traffic during high-use periods. Provision servers accordingly and conduct load tests ahead of time to be sure that the infrastructure can handle the additional traffic.

Ensure that your website is protected against DDoS attacks and monitor traffic to detect anomalies. Free DDoS protection and mitigation services are available, such as Google's Project Shield and Cloudflare's Athenian Project.

Detect

Have a dedicated person with the job of looking for fake content or spoofed websites in search engine results.

Recover

Have a backup version of the website hosted elsewhere in case the primary site goes down. This version should contain only barebones, essential information (e.g., precinct locations / hours).

Vendor Considerations

Official websites are often created by vendors, and in many cases vendors are also responsible for making changes to them.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Social Media (official and private accounts)

KEY THREATS:

Account compromise: Attackers use spear-phishing to learn the username and password for the county Facebook page which did not have two factor authentication enabled. The attackers then post misinformation about certain voting sites having several hour wait times and direct voters to alternate sites which are then overwhelmed.

Fake accounts: Malicious actors create a fake Twitter account for an election official (e.g., Secretary of State, Election Director) which gains traction because it is retweeted by a bot farm controlling several thousand accounts. The fake account then posts the wrong unofficial election results after polls close.

Recommended actions:

Identify

Be cognizant of which accounts could be used to disseminate information about an election. This includes accounts for your organization, as well as both the professional and personal accounts for officials. Determine who has access to each of these accounts.

Identify points of contact and establish relationships with key social media firms like Facebook and Twitter. Confirm a point of contact in case social media accounts connected to the election are compromised; or in case malicious fake accounts surface. Confirm the requirements for regaining control over accounts and shutting down malicious fake accounts.

Know key stakeholders for communication channels (media, political party contacts, advocacy groups, etc.)

Protect

Inform key officials that their private accounts might be targeted. Establish clear policies for officials and staff on use of private accounts for sharing official information, including policies for communicating indications of malicious cyber activity.

Secure social media accounts. Social media services such as Twitter and Facebook support two-factor authentication for accounts, and enabling this capability is the best step you can take to keep your accounts secure and should be done for both official accounts and the personal accounts of key personnel. In addition to this, require that the passwords for your official accounts be secure.

Understand third-party apps can be a vulnerability if they are compromised. Use third-party social media management platforms judiciously to reduce your threat surface. Periodically review linked accounts and connected apps and remove any that are no longer required.

Detect

Have a dedicated person responsible for looking for fake content in search engine results or on social media.

Recover

See the **Election Cyber Incident Communications Playbook** and **Election Cyber Incident Communications Plan Template** *for State and Local Election Officials*.

Engage with social media firms to recover/disable accounts.

If an account has been compromised, review what permissions it has granted to third-party apps and reset them to prevent further access by unauthorized parties.

Vendor Considerations

If you need to use a third-party social media application to manage social media accounts, then research the applications security practices and access policies to understand what vulnerabilities using it presents.

Vendor Considerations

*(See **Appendix 1, Vendor Selection and Management**, for best practices related to vendor contracts.)*

1. **Clearly define** the division of labor and responsibilities between the vendor and the local officials. Identify any gaps between the two parties and specifically assign responsibility to fill those gaps.
2. **Create and enforce contractual requirements.** Require vendors to adhere to well-defined security practices ensuring safe handling and protection of data.
3. **Require vendor assessments.** State/local contracts with vendors should include provisions requiring vendors to conduct third-party vulnerability assessments of their systems and share the results. See vendor appendix for more details.
4. **Mandate that vendors permit penetration testing of systems**, including voting machines, as part of RFP contracts.
5. **Secure access.** Unnecessary personnel should not have access to systems. Vendors who need access to secure systems should be granted temporary credentials and exercise that access under the supervision of a state or county official. Once a developer has finished building an application, ensure that they do not have access to the production system.
6. **Secure data transmissions.** Require vendor systems to use digital signatures to ensure the integrity of all received and transmitted files.
7. **Require audit logs for any vendor-run system.**
8. **Mandate patching** as part of a vendor request for proposal (RFP) contracts and ensure that the patching is conducted securely and frequently.

Appendices

Appendix 1. **Vendor Selection and Management**

Election system vendors are key partners in addressing cybersecurity risks. Their systems, by definition, increase the attack surface and present additional risk factors that must be mitigated to address cyber threats. Since vendors often develop and maintain systems critical to elections (such as ballot counting equipment and VRDBs), it is crucial to ensure that their protocols and practices meet rigorous cybersecurity standards.

Performing a security risk assessment of vendors during the request for proposal (RFP) process can reveal vendor vulnerabilities and reduce future exposure to external attacks. This risk assessment should be conducted in two steps: 1) during the procurement process, ensure that all vendors are willing and able to comply with security standards that meet, or exceed, election agency expectations, and 2) validate vendors' ability to meet their commitments via thorough due diligence, and ensure that vendors are reviewed periodically, not just at the time of selection.

When assessing a vendor, there are three general principles to consider:

> **Organizational security practices.** Evaluate the extent to which cybersecurity activities and outcomes are embedded across the organization, from the executive level to the implementation/operations level, such as hiring, subcontracting, policies and procedures, cybersecurity awareness and training, network and system management, vendor management, vulnerability management, and software/hardware development.

> **Ongoing partnership capacity.** Vendors should be your partners in addressing cybersecurity risks! Evaluate the levels of transparency associated with their cybersecurity processes, and to what extent they will collaborate with you on key security risk-mitigation activities, including consequence management after a cyber incident. These would include code reviews, vulnerability scans, patching, and implementing controls to strengthen their security posture, while also closing critical gaps.

> **Maintenance strategy.** Cybersecurity is not a "point in time" activity and you may have a long-term relationship with a vendor. As new attacks emerge, software and hardware should be updated commensurate with the nature of evolving risks and the state of the art in cybersecurity safeguards. This expectation must be built into vendor contracts.

Specific security requirements for vendor agreements

With the above principles in mind, security requirements should be clarified in RFPs to ensure that vendors are limiting cyber risks while working with the states or counties. The following set of core security requirements are not exhaustive, but they do provide a foundation to include in vendor RFPs. Each vendor bidder should be required to:

- State how system access in the proposed solution will be managed.
- Describe what type of data will be processed and how it will flow through the system, including any relevant data processing or data storage vendors and, if applicable, locations.
- Describe security at all layers of the solution—application, server, database, data exchange, and network security layers should all have the ability to manage access and privileges at a granular level.
- Describe how security measures will protect data for the entire data life cycle, ensuring that data remains protected for as long as it is in the control of the vendor and, when required, is securely destroyed.
- Describe how the proposed solution meets or exceeds compliance with all state- or county-level security requirements.
- Describe how encryption will be implemented for data "at-rest" and "in-transit."
- Describe how User Access Management will be handled under the principle of "least privilege" (i.e., provide only the minimum level of access required for the user to perform his or her core job), as well as how it will be maintained and pared over time.
- In your Service Level Agreements (SLAs), include clauses for vendors to notify you in the event of a cybersecurity breach of their systems or other unauthorized access immediately after they become aware and to cooperate with any consequential investigation, response, and mitigation.

Transparency requirements should also be established in the RFP to ensure that officials have the ability to perform due diligence and conduct independent security risk assessments. Moreover, transparency will aid in identifying potential conflicts of interest. Non-Disclosure Agreements will protect vendor proprietary information, in exchange for receiving access to:

- **Corporate governance relating to security practices.** Officials should have the ability to review vendors' security policies, standards, and guidelines. They should be able to assess whether these are implemented in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

Internal security audits. State officials should perform audits (and retain the right to do so) of a vendor's security practices and protocols. This activity provides assurance that the vendor's cybersecurity practices are robust and meet state and local security standards, including those outlined in the above section. This is especially important in the months and years after vendor contracts are signed. Vendor-provided system logs should be contractually viewed as customer owned data not vendor owned data. For instance, voting system audit logs should be readily available to election officials and considered by contract as their data.

Source code. Election officials should have access to the source code for any critical system to perform internal or third-party reviews. This can be a sensitive subject because of intellectual property concerns, but being able to independently audit vendor-created code allows officials to ensure that the code is secure. It also guarantees that the code does not contain any potentially unwanted networking requests, transfers of sensitive information, or modifications to key algorithms and counting mechanisms.

Penetration testing. Penetration testing is a critical element in ensuring that vulnerabilities in vendor environments are proactively identified and closed. The RFP should clearly include requirements for the vendor to allow penetration-testing by state officials or third parties of their systems to discover weaknesses. Vendors may resist these provisions, especially if they hold broader state contracts that could be affected if vulnerabilities are discovered. Nonetheless, conducting these tests represents the best way to identify cracks in critical infrastructure before malicious actors do, and should be part of any contract with vendors who work on and maintain these systems.

Data flow transparency. Officials should have full visibility into data flows for voting system data. Therefore, it is essential for officials to request that the vendor provide its applicable data retention and destruction policies, a list of relevant physical locations where data will be processed, stored, or otherwise accessed, and an exhaustive list of subcontractors who may process, store, or otherwise access voting data or systems. Depending on the nature of the vendor's services, it may be necessary to impose flow-down security and audit requirements on subcontractors, including on the vendor's infrastructure vendors, or, if relevant, to explicitly restrict data storage locations.

Appendix 2. **Election Audits**

While following cybersecurity best practices will help deter and defend against malicious actors, there is no such thing as an impenetrable system. Even if an election system is not attacked, software or hardware errors could lead to an incorrect vote tally. To protect against technical manipulation or failures undermining the process, elections should be "software independent," meaning that they do not rely on a computer to provide a vote count, but instead have an independent auditable paper record for definitive results.

You should conduct a post-election statistical audit with these paper voting records. Such audits provide two critical benefits: (1) they offer transparency and build public confidence in the system and process; (2) they confirm the accuracy of the results, or, on rare occasion, identify that an error has occurred and must be addressed. Post-election audits are designed to be an independent confirmation of the election result. These audits should be observable and reproducible by external third parties. This requires making data necessary to conduct the audit publicly available to independent parties so that they can confirm audit results.

There are two main methods of post-election audits. Since performing a full hand-count of every ballot is extremely time-intensive and the results will likely be inaccurate, other methods are used to inspect the results with a manageable amount of work.

The first audit type uses a fixed percentage of ballots cast. This method, however, can overestimate or underestimate the necessary number of ballots required for a successful audit. In the overestimation case, the audit is inefficient and a waste of resources; in the underestimation case, the audit doesn't fulfill its purpose. That said, a fixed percentage audit is still better than no audit at all and is regarded as a "good" standard of practice.

The second type is the statistical audit where statistical methods are used to determine and inspect the minimum number of ballots required to confirm that an election has not been altered—this would be considered an "enhanced" standard of practice. As the margin of victory between the winner and loser narrows, more ballots are required to ensure an accurate audit. Typical implementations of statistical audits could require multiple rounds of ballot inspection if discrepancies are found with recounted ballots. If the statistical audit fails, a full recount of all ballots is necessary to ensure the election has not been compromised.

The following section discusses the “good” and “enhanced” audit techniques: (1) *Good:* fixed-percentage audits; (2) *Enhanced:* risk-limiting audits with two variants (a) comparison audits, and (b) ballot-polling audits.

Fixed-Percentage Audits

Fixed-percentage audits provide some evidence that results are valid. One example process: Counties indicate to the Secretary of State (or State Election Director) which machines they will use in the election, then the Secretary of State (or Election Director) randomly selects one DRE and one optical ballot scanner per county. The county must then audit a fixed percentage (e.g., 20 percent) of the ballots tallied by the optical scanner, as well as manually counting all the paper vote records produced by the DRE and comparing this number to the DRE’s electronic vote count. This process ensures that, for the randomly selected machines, the pre-election logic and accuracy tests were successfully conducted, a chain-of-custody was maintained, and the devices functioned properly on election day. The weakness of a fixed-percentage audit is that specific devices, rather than the election itself, are audited. Election officials cannot be certain that the election as a whole was conducted correctly, but this may be the best available option for some counties with limited resources or technology.

Risk-Limiting Audits (Enhanced Statistical Methods)

The first step in any risk-limiting audit is setting the risk limit. Setting a 5 percent limit means that if an audit is conducted on an election that did, in fact, experience tampering, there is at most a 5 percent chance that the audit will not discover the error and at least a 95 percent chance that the audit will find the election outcome to be manipulated. The number of ballots required for a risk-limiting audit is determined by the risk limit and margin of victory. A closer election or lower limit requires more ballots to be audited. There are two types of risk-limiting audits: (1) comparison audits and (2) ballot-polling audits.

> A. **Comparison vs. Ballot-Polling Audits.** A comparison audit involves recounting a randomly selected set of ballots and comparing those results with the original machine-recorded tabulation of those exact ballots, called the Cast Vote Records (CVRs). Comparison audits are typically recommended over ballot-polling audits for greater efficiency. Unlike a ballot-polling audit, a comparison audit requires knowing the original tabulation results of the specific ballots you are auditing (in the CVR) and comparing

discrepancies. A ballot-polling audit simply looks at the outcome of the ballots inspected. Because of this precision, comparison audits require far fewer ballots to be counted than do ballot-polling audits. However, comparison audits require specific data (machine tabulation and associated paper vote record from a given voting machine), which may be infeasible for some counties.

B. **Audit Level.** Audits can operate on different levels depending on the infrastructure available. A unit could be a single ballot, a batch of ballots, all the ballots processed by a machine or all the ballots in a given precinct. For a given unit, samples are typically selected randomly then the ballots within that unit are inspected. For statistical risk calculations, the larger the unit, the larger the total number of ballots that will need to be inspected to have the same risk of missing an incorrect outcome. Ballot-level comparison audits are most efficient in terms of number of ballots considered for a given margin of victory and risk limit because they spread the audit across many ballots in multiple precincts. This means this audit is more likely to find any election meddling. Batch, machine, or precinct level audits require doing a comparison audit on batches of ballots only at certain precincts. This is less likely to find election meddling and requires auditing more ballots to ensure the same level of confidence that an election outcome is true, but may be more feasible for some counties.

There has been extensive research on this issue by leading experts in the field of election auditing. The following reports can provide additional information:

- "A Gentle Introduction to Risk Limiting Audits" Mark Lindeman and Philip B. Stark
- "Bayesian Tabulation Audits: Explained and Extended" Ronald L. Rivest
- "On the Notion of 'Software-Independence' in Voting Systems" Ronald L. Rivest and J.P. Wack
- "Evidence-Based Elections" by Philip B. Stark and D.A. Wagner

External Resources Guide

There are many threats that could undermine the democratic process; fortunately, election officials are not in this alone. There are resources available that can help defend against those threats, including free ones.

Federal Support

The Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) offers a variety of services at no cost or minimal cost for states and counties. Services include:

1. Cyber Hygiene checks, which scan election and other Internet-accessible systems (such as public-facing VRDB portals) for vulnerabilities and configuration errors. DHS can also provide a report that outlines steps to address or mitigate vulnerabilities detected in the scan.
2. Risk and Vulnerability Assessments (RVAs), which involve DHS teams performing in-depth on-site analysis of a state or local election facility's internal and external networks. RVAs can include penetration testing, vulnerability scanning and testing, database and operating systems scans, Web application scanning and testing, and several other services.
3. The National Cybersecurity and Communications Integration Center (NCCIC) is a cybersecurity situational awareness, incident response, and management center that operates 24 hours a day, 7 days a week. NCCIC collaborates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to State and local governments.
4. MS-ISAC disseminates early warnings on cyber threats to state and local governments as well as security incident information and analysis through a 24-hour security operations center. MS-ISAC also provides intrusion detection.
5. Cyber Security Advisors (CSA) and Protective Security Advisors (PSA) are security professionals deployed in all 50 states to provide direct assistance, such as vulnerability assessments, and reach-back to additional government resources and capabilities.

Private Sector Support

For defending election system-related public-facing websites, Google's Project Shield and Cloudflare's Athenian Project are free services that defend websites from distributed denial of service (DDoS) attacks. Other software development firms are developing free open source software to assist states and localities in conducting risk-limiting audits. Several highly experienced cybersecurity firms also offer penetration testing and risk vulnerability assessments.

National Guard Collaboration

The National Guard is building cyber units in many states and territories. These units align with the Army and Air Force. When not performing their federal mission, these units may be available for state-specific tasking under state authorities. Several states have employed their National Guard cyber capabilities to participate in activities such as vulnerability assessments and penetration testing.

Recognizing that there are Constitutional and legal sensitivities, states interested in exploring opportunities with their National Guard units should work through their governor's office and ultimately their state's Adjutant General office. If states do not have a resident National Guard cyber capability, they can potentially partner for support with nearby states who do have this resource. In some cases, support can be provided through the Emergency Management Assistance Compact (EMAC) process, similar to other civil support capabilities. These compacts act as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance. A useful analogy is to consider National Guard support in cyberspace in a similar light as the laying of sandbags before a storm in the physical world.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

What Every Election Staffer Should Know About Cybersecurity

1. **Everyone is a security official**
   Take cybersecurity seriously. Take responsibility for reducing risk, training your staff, and setting the example. Human error is the number one cause of breaches. Spear-phishing attacks and other attempts at interference can be thwarted with cybersecurity vigilance.

2. **Use two-factor authentication (2FA)**
   Use two-factor authentication for everything: official work accounts, personal email accounts, social media accounts, and any data storage services. Use a mobile app (such as Google Authenticator, Duo, or Authy) or a physical key (such as Yubikey or other U2F devices) for your second factor, not text messaging. 2FA is an extra step, but is very effective at preventing unauthorized access.

3. **Create long, strong passwords**
   Current computing capabilities can crack a seven-character password in milliseconds. For your passwords, create **`SomethingReallyLongLikeThisString`**, not something really short like **`Th1$`**. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of **`$ymB01$`**.

4. **Keep credentials secure**
   When collaborating with others, resist the temptation to share credentials to systems with them, regardless of who they are.

5. **Practice cyber hygiene**
   Follow all applicable guidance for patching and software updates. Ensure that your systems have the most updated antivirus software.

Glossary

Based on the Election Assistance Commission's Common Cybersecurity Terminology and Information Technology Terminology Glossaries

Cybersecurity Terms:

Access
Ability to make use of any information system (IS) resource.

Access control
The process of granting or denying specific requests: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities.

Advanced Persistent Threat
An adversary who possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

Asset
A major application, general support system, high impact program, physical plan, mission-critical system, personnel, equipment, or a logically related group of systems.

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Attacker
A party who acts with malicious intent to compromise an information system.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backups
A copy of files and programs made to facilitate recovery if necessary.

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Blacklist
A list of entities that are blocked or denied privileges or access.

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected information.

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Critical infrastructure
System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, national public health or safety, or any combination of those matters.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Loss
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Decryption
The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Denial of Service
The prevention of authorized access to resources or the delating of time-critical operations.

Encryption

The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it. Encryption does not prevent interception, but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down. Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

Firewall

The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Hack

Unauthorized attempt or access to an information system.

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Incident Response Plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information systems(s).

Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Multi-factor Authentication

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something that identifies who you are (e.g., biometric).

Password

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch

An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Port

The entry or exit point from a computer for connecting communications or peripheral devices.

Port scanning

Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Private key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key or to decrypt information which has been encrypted using the public key.

Risk analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls that are planned or in place.

Spear Phishing

A colloquial term that can be used to describe any highly targeted phishing attack.

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system.

Structured Query Language (SQL) injection
An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Tabletop Exercise
A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Threat
Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Unauthorized access
Any access that violates the stated security policy.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

General Information Technology Terms:

Air Gap

An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called "Sneaker Net." Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Audit

A review of a system and its controls to determine its operational status and the accuracy of its outputs. Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail

The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication

The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Blacklist

A list of URLs, domains, users, or other identifiers, that have had system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Code

n. Synonym for program or software.

v. to create or modify software.

Data destruction

The removal of data from a storage medium. Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database

A structured collection of data that includes data and metadata (data about the data). Databases are managed by database management systems. The election database stores all of the requisite information to manage election including precinct information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Download

Transferring data from a larger computer to a smaller computer or device. An EMS facilitates downloading ballot images to vote capture devices.

Dox

Publish damaging or defamatory information about an individual or organization on the Internet. One method of hacking a campaign is doxing (or doxxing).

File

A collection of related data, stored on media. Files will be identified by a system-valid filename.

Firewall

A gateway computer and its software that protects a network by filtering the traffic that passes through it. Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the Internet.

Two-factor Authentication

Authentication mechanism requiring two or more of the following: something you know (e.g., Password), something you have (e.g., Token), something that identifies who you are (e.g., biometrics).

Penetration Testing

Also called Pen Testing. An evaluation method that enables a researcher to search for vulnerabilities in a system. Election systems, such as the VR system, are periodically submitted to a Pen Test to determine their vulnerabilities to cyber attacks.

Ransomware

Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device. Election office computers should maintain high levels of cyber hygiene, including up-to-date anti- malware systems and adherence to best practices regarding managing browser and email client activities.

Social Engineering

Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech. Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software

A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer. The Election Management System (EMS) used to create election databases is software.

Spear Phishing

A targeted attack by hackers, via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors. Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Software Patches

Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes. Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise

A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning. Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Wi-Fi

Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections. Some e-Pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Election Administration Technology Terms:

Central Count Optical Scan

Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies. Central count systems lack overvote/undervote protection capabilities.

Digital Optical Scan System

Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems.

Direct Record Electronic Voting System (DRE)

A DRE system presents a ballot image to a voter, collects the voter's choices, and records those choices directly onto electronic media. DREs may be fitted with VVPAT subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction and image displays, and can hold a large number of ballot styles in multiple languages.

Election Night Reporting Systems (ENR)

A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near-real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Poll Book (EPB)

Hardware and/or software that permits election officials to review the electors list and mark voters who have been issued a ballot. Also called an e-Pollbook. E-Pollbooks can be standalone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

High-Speed Central Count Tabulation System

An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Optical Scan System (Op Scan)

A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan

Optical scan technology that permits voters to mark their paper ballots within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Risk-Limiting Audit

Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Voluntary Voting System Guidelines (VVSG)
Collection of standards that is developed and maintained by the EAC. The VVSG specifies a minimum set of performance requirements that

Voter Verified Paper Audit Trail (VVPAT)
Contemporaneous paper-based printout of voter choices on a DRE.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P

National Association of Elections Officials
Election Center
Elections Security Checklist

May 2017

ELECTION CENTER

21946 Royal Montreal Drive, Suite 100, Katy, TX 77450 281-396-4309

Elections Security Checklist

Identify and Assess Critical Election Systems	
1.) Have you defined your inventory of critical election systems? *(for example, the Voter Registration Database; Websites like your Voter Data Lookup Tool; Election Tally System; Voting Machines, etc.)*	□ YES □ NO
2.) For each system, do you regularly assess the value of the information contained within, the necessity of perfect functioning of the system, and potential risks to it?	□ YES □ NO
3.) For each system, are you actively cataloging it and building/improving defenses to protect it?	□ YES □ NO
4.) For each system, have you developed a plan to recover should disaster strike?	□ YES □ NO
For each system identified, engage in the following critical analysis to assess the relative risks, defenses, and recovery plans you have in place.	
I. Risk Assessment **(Complete a Risk Assessment for every system)**	
A. Physical Security Risk	
1.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election headquarters?	□ YES □ NO
2.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election warehouse?	□ YES □ NO
3.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your server room or data center?	□ YES □ NO
4.) Have you examined your physical access authorization policy in the last three months?	□ YES □ NO
5.) Do you perform scheduled audits of authorized personnel prior to each election?	□ YES □ NO
6.) Do you reexamine your physical access policies on any regular schedule?	□ YES □ NO

A. Physical Security Risk (con’t)	
7.) Have you ever conducted a test to see if your facilities can be entered by unauthorized personnel?	❏ YES ❏ NO
8.) Do you have policies and procedures in place for intrusion incident response?	❏ YES ❏ NO
9.) Do you have surveillance cameras in place at key facilities?	❏ YES ❏ NO
10.) Do you have a system in place that automatically identifies suspicious behavior as seen on the surveillance system and creates a management alert?	❏ YES ❏ NO
11.) Do you regularly review your video if there is not a system to automatically identify suspicious behavior?	❏ YES ❏ NO
B. Network Security Risks	
1.) Do you have a complete map of your network and all its interconnections, both within your organization and with outside entities?	❏ YES ❏ NO
2.) Do your vendors and partners have a strong commitment to network security?	❏ YES ❏ NO
3.) Have you reviewed your vendors and partners’ written plans and checkpoints that demonstrate implementation?”	❏ YES ❏ NO
4.) Do you have a map of the data elements that pass between each application system on your network and with outside entities?	❏ YES ❏ NO
5.) Are all of your network connections to outside entities secured by a Virtual Private Network (VPN) or something comparable?	❏ YES ❏ NO
6.) Is there any group or department within your organization whose mission is to monitor network security?	❏ YES ❏ NO
7.) Have you developed a worst case scenario for potential damage if an unauthorized person gains access to any part of your network?	❏ YES ❏ NO
8.) Do you have anti-virus software installed to detect “Advanced Persistent Threats”?	❏ YES ❏ NO
9.) Does any outside entity, such as a statewide voter registration system, have the ability to alter or delete data from any of your internal systems?	❏ YES ❏ NO
10.) Do you regularly conduct vulnerability and intrusion testing on your network?	❏ YES ❏ NO

C. Software Applications Security Risks *(Note: Systems may have numerous applications that touch them. For example, a voter registration system may be composed of a voter database application, and also connected e-poll book software application, and connected statewide voter database application. Running the application level analysis on each of the program level applications will give you your best sense of your security and preparedness.)*	
1.) Application (insert name) Security Risks (repeat a, b, c and d questions for every security risk application)	
a.) Information at Risk	
1.) Does your application house any information not subject to public disclosure? *(for example, any personally identifiable information (PII) such as SSN, Driver's license, date of birth, etc.)*	❑ YES ❑ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❑ YES ❑ NO
3.) Does this application share, transmit, or receive information with any other application or system?	❑ YES ❑ NO
4.) Does this application house any data that affects election results?	❑ YES ❑ NO
5.) Does this application have any type of network or internal system connection with any application that affects election results?	❑ YES ❑ NO
6.) Does this application house any data that is essential to the running of an election, and without which the election would either be impossible to administer or whose results might be questioned?	❑ YES ❑ NO
b.) Acceptable Use Policy	
1.) Do you have a written policy for this application describing who may use it and under what circumstances?	❑ YES ❑ NO
2.) Do you have an enforcement mechanism and management review process in place to ensure compliance with any such policy?	❑ YES ❑ NO
3.) Is your acceptable use policy implemented in software in such a manner that your systems enforce the policy?	❑ YES ❑ NO
c.) Worst Case Scenarios	
1.) If this application or its database were completely destroyed or disabled at a critical time, could you still conduct your election?	❑ YES ❑ NO

c.) Worst Case Scenarios (con’t)	
2.) Even if you could conduct the election, would public confidence in the results be maintained? *(for example, a hacker had cancelled a large number of voter registrations for one competing party)*.	❏ YES ❏ NO
3.) Could you still ensure that no voters would be disenfranchised as a result of the application problem? *(for example, excessively long lines, or unavailable registration information, or for some other reasons)*.	❏ YES ❏ NO
II. Defense Layers	
A. Physical Defenses	
1.) Is physical access to your site restricted to authorized users?	❏ YES ❏ NO
2.) Is there site security staff at the location(s) where your system is located?	❏ YES ❏ NO
3.) Is there a log of the identities and access times of individuals physically accessing your site?	❏ YES ❏ NO
4.) Is your site security staff present at times when staff are not present?	❏ YES ❏ NO
5.) Are all entrances (including windows, etc.) secured by alarms and/or security cameras?	❏ YES ❏ NO
6.) Does your management regularly review physical security records such as logs, video footage, alarm notifications, etc.?	❏ YES ❏ NO
7.) Is the data center where your computer servers are located physically protected in the event of fire, terror attacks or flooding?	❏ YES ❏ NO
8.) Do you have a backup site available if any of your facilities become suddenly inoperable during a critical period?	❏ YES ❏ NO
9.) Have you determined how long it will take to get the backup site functioning? (including the determination of any loss of data).	❏ YES ❏ NO
10.) If any of your computer systems are housed in a vendor-supported data center, has that vendor supplied you with a detailed description of their physical security, fire protection, backup and recovery procedures?	❏ YES ❏ NO
11.) Are your temporary workers required to wear ID badges or other identification so that unauthorized persons in your facilities can be quickly spotted?	❏ YES ❏ NO

B. Network Defenses	
1.) Is there an “air gap” between the Internet and your election tally system *(i.e. is your tally system physically disconnected from the Internet)*?	❏ YES ❏ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❏ YES ❏ NO
3.) Are your public-facing voter systems, e.g. a “check my registration” application, built using copies of critical information rather than being directly connected to critical information databases?	❏ YES ❏ NO
4.) Do you review your network activity logs daily?	❏ YES ❏ NO
5.) Do you review your logs at least once a week?	❏ YES ❏ NO
6.) Do you have any User & Entity Behavior Analytics (UEBA) software running on any of your critical infrastructure that can alert you to suspicious network activity?	❏ YES ❏ NO
7.) Do you conduct any periodic vulnerability, intrusion and penetration testing on your networks?	❏ YES ❏ NO
8.) Do you create and store daily application system back-ups?	❏ YES ❏ NO
9.) Do you transfer data to or from the isolated network using a specified USB device that is used only for that purpose and verified to be clean?	❏ YES ❏ NO
10.) Do you have a network access control system that controls user access permission levels? *(e.g. Microsoft Active Directory)*	❏ YES ❏ NO
11.) Do you control access to any of your systems by outside organizations or individuals by using Virtual Private Networks (VPNs)?	❏ YES ❏ NO
12.) Is your network password-protected?	❏ YES ❏ NO
13.) Do you provide administrative passwords only to employees with a clearly defined “need to know/edit” status?	❏ YES ❏ NO
14.) Do you change critical system passwords regularly *(recommendation every 90 days)*?	❏ YES ❏ NO
15.) Do you ensure that servers, PCs and laptops are encrypted or updated with the most current security patches?	❏ YES ❏ NO
16.) Do you ensure the organization has the most current versions of virus protection software?	❏ YES ❏ NO

C. Software Applications Defenses	
1.) Application (insert name) Defenses **(repeat a., b., c., d questions for every software defense application)**	
a.) Data Protections	
1.) Are only authorized personnel granted access to the software?	❏ YES ❏ NO
2.) Is this application set up with different, unique passwords for each user?	❏ YES ❏ NO
3.) Is this application set up with different passwords for different elections?	❏ YES ❏ NO
4.) Is this application set up with robust passwords *(passwords include special characters and caps-best practices recommends changing passwords every 90 days)*?	❏ YES ❏ NO
5.) Is this application set up with tokens or other special access rights?	❏ YES ❏ NO
b.) Software level application level protections	
1.) Is the software platform protected by a firewall?	❏ YES ❏ NO
2.) Is the software platform isolated in the network environment?	❏ YES ❏ NO
c.) Software Logs	
1.) Does the software log the user name, time, date, and type of modification?	❏ YES ❏ NO
2.) Does the software log multiple log-in attempts, increased data traffic, and/or volume of data transmitted?	❏ YES ❏ NO
d.) User & Entity Behavior Analytics (EUBA)	
1.) Do you have baseline measurements for “normal” activity patterns within this application and an alert system that identifies abnormal activity patterns?	❏ YES ❏ NO
III. System Disaster Recovery	
A. Physical Disaster Recovery	
1.) Is there backup for the loss of hardware *(networks, servers, computers and laptops, wireless devices)*?	❏ YES ❏ NO
2.) Is hardware available at an alternate facility that can be configured to run similar hardware and software applications when needed?	❏ YES ❏ NO
3.) Is there backup for the loss of impounded voting equipment?	❏ YES ❏ NO

A. Physical Disaster Recovery (con’t)	
4.) Is there a contingency for natural disasters or homeland security breach for data contained at data center?	❑ YES ❑ NO
5.) Are there plans for relocating Receiving Stations (where poll workers return election night supplies) in the event of a natural disaster or homeland security breach?	❑ YES ❑ NO
6.) Is there backup for the loss of data from election equipment damage?	❑ YES ❑ NO
7.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
8.) Is there ready access to your alternative physical locations?	❑ YES ❑ NO
9.) Is there a timeframe in place for the alternative facility to be functioning?	❑ YES ❑ NO
B. Network Disaster Recovery	
1.) Is there a plan for providing automatic redirects for interfaced systems should you need to move your system to a new network location?	❑ YES ❑ NO
2.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
3.) For the backup hardware and networking plan, is there necessary staff available during critical periods?	❑ YES ❑ NO
C. Software Applications Disaster Recovery	
1.) Application (insert name) Disaster Recovery **(repeat a., b., c., d questions for each software disaster application)**	
a.) Damage Assessment	
1.) Are vendors on standby for critical periods to assist with Assessment and Disaster Recovery?	❑ YES ❑ NO
2.) Are you able to run a hash comparison with the recovery (i.e. back-up) copy of your software application?	❑ YES ❑ NO
b.) Data Restore	
1.) Are your backup disks or file locations readily accessible?	❑ YES ❑ NO
2.) Are your backup files saved in an off-site location?	❑ YES ❑ NO
3.) If you have a parallel application running, is it up to date?	❑ YES ❑ NO

c.) Application Restore	
1.) Do you have necessary staff or vendor resources available to assist with the installation of the application in a mirrored physical and OS environment?	□ YES □ NO
d.) Business Restore	
1.) Are you prepared to cut over to alternative applications that can manage limited business critical functions? *(For example, if your Voter Registration System crashes, can you quickly utilize your web based voter search application so that you can direct voters to their polling place on Election Day?)*	□ YES □ NO
2.) Are there paper alternatives to allow you to continue with on-going critical processes while technical systems are diagnosed and brought back? *(For instance, do your voting machines create countable paper trails viewable by each voter?)*	□ YES □ NO
3.) Can you quickly create paper voter lists in the event e-poll books go down?	□ YES □ NO
The Election Center would like to acknowledge and thank the committee that worked on the initial draft of this checklist: Noah Praetz, Cook Co. IL; Dean Logan, Los Angeles Co. CA; Jennifer Morrell, Arapahoe Co. CO; Janice Case, King County, WA; Eric Fey, St. Louis Co. MO; Brian Corley, Pasco Co, FL and Ryan Macias, U.S. EAC	

Voting System Technical Oversight Program at Ball State University (VSTOP)

Indiana Best Practices Manual for the Operation of Election Equipment

June 2018

Indiana Best Practices Manual for the Operation of Election Equipment

JUNE 25, 2018

Voting System Technical Oversight Program

VSTOP

Indiana Best Practices Manual
for the Operation of Election Equipment

Prepared by
Voting System Technical Oversight Program
(VSTOP)
Bowen Center for Public Affairs
Ball State University

Version 1.1
June 2018

Version History

Date	Version Number	Description
March 28, 2018	1.0	Original draft version
June 4, 2018	1.0	Revised draft version
June 25, 2018	1.1	Revised

Table of Contents

1. Introduction

Since the Help America Vote Act (HAVA) was passed by the United States Congress in 2002, Elections and Voting Systems have changed considerably. Today's voting systems are totally dependent on Information Technology and, according to the United States Election Assistance Commission (EAC) publication *Ten Things to Know About Selecting a Voting System*, *Managing Election Technology Series #1* [1], the "Election Official of today is an Information Technology (IT) Manager."

IC 3-5-2-53 incorporates this definition of voting system as follows:

IC 3-5-2-53 "Voting system"
Sec. 53. "Voting system" means, as provided in 52 U.S.C. 21081:
(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support that equipment) that is used:
(A) to define ballots;
(B) to cast and count votes;
(C) to report or display election results; and
(D) to maintain and produce any audit trail information; and
(2) the practices and associated documentation used:
(A) to identify system components and versions of those components;
(B) to test the system during its development and maintenance;
(C) to maintain records of system errors and defects;
(D) to determine specific system changes to be made to a system after the initial qualification of the system; and
(E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).
As added by P.L.4-1991, SEC.5. Amended by P.L.209-2003, SEC.3; P.L.164-2006, SEC.2; P.L.128-2015, SEC.5.

Additionally, HAVA also established the EAC and prescribed the development of Voluntary Voting System Guidelines (VVSG) to help the States test, certify and implement voting system hardware and software. The State of Indiana requires, among other conditions, that voting systems certified in the state be VVSG compliant. The Voting System Technical Oversight Program (VSTOP) works with the state to manage the testing and certification of voting systems. VSTOP has also developed the "Indiana Electronic Poll Book (ePB) Certification Test Protocol" [2] for certification and testing of electronic poll books (ePBs) used in Indiana.

This **Indiana Best Practices Manual for the Operation of Election Equipment ("Manual**") has been designed with you, the County level election official, in mind. This Manual will also be useful to poll workers and other involved in conducting elections. VSTOP's goal in bringing this manual to you is to provide a collection of the current set of best practices in the operation of voting systems, ePBs, cybersecurity, and physical security of election equipment and materials.

The scope of this Manual is limited to the collection of best practices described above. This Manual is not designed to replace the operations manuals of your county's voting systems and/or electronic poll books. Rather, this Manual is a set of general best practices that apply to all types of voting equipment (including electronic poll books). These best practices are in addition to the best practices that may be included in the operating and training materials that came with your election equipment.

This Manual includes the following Sections.

The section on *Best Practices for the Operation of Voting Systems* includes general best practices that apply to any type of voting system and associated equipment and materials.

The section on *Best Practices for the Operation of Electronic Poll Books* includes general best practices that apply to ePBs and their functionality.

The section on *Election Cybersecurity Best Practices* covers cybersecurity related best practices that apply to all aspects of conducting elections, including the use of voting equipment, while the section on *Elections Physical Security Best Practices* covers similar aspects for physical security of election equipment and related materials and resources.

The section on *Standards and Best Practices based on Indiana Election Code* includes a discussion of Indiana statutes that apply to physical and cybersecurity aspects of elections and election equipment. This section may be expanded in future versions to include similar federal election statutes.

VSTOP has consulted many resources to compile the information in this Manual. These resources include the National Institute of Standards and Technology (NIST), The Belfer Center, Harvard Kennedy School, U.S. Election Assistance Commission, National Conference of State Legislatures (NCSL), and the Indiana Department of Homeland Security.

A complete list of those resources is included in the *Resources* section. We recommend that you consult these resources as often as needed and check these regularly since new information is regularly added. Hyperlinks are provided where available.

The Manual concludes with a *Glossary* and a set of *End Not*es that include the collection of references used in this Manual.

It is our expectation that this Manual will undergo frequent revisions and updates. We expect to provide the most recent version in a downloadable format. For more information please contact the VSTOP Team at vstop@bsu.edu.

We value your questions, feedback and suggestions for changes and additions. Those will help us improve future versions of the Manual. Please write to us at vstop@bsu.edu.

2. Best Practices for the Operation of Voting Systems

This section presents best practices for voting system operation. These best practices apply to all voting systems and are not vendor specific. We group the best practices into several categories.

Best Practices for Keeping your Voting System Up-To-Date:

- Know the certification status of all your voting system equipment (this may be done by referring to your inventory in the VSTOP-ESI inventory database or by referencing similar information on the IED/SOS website).
- Monitor technical bulletins from your vendor. Ask your vendor about any known or new issues.
- Monitor changes to your voting system such as modifications and engineering change orders (ECOs). You may ask your vendor about any changes, contact VSTOP for the information or refer to the VSTOP-ESI inventory database.
- Follow your vendor's manuals and best practices for voting system operation.
- Keep a record of your voting system's maintenance.
- Follow your vendor’s guidelines for environmental requirements for storage and transportation of voting equipment and peripherals/accessories.

Best Practices for Aging Voting Systems: The EAC publication, 10 Things to Know About Managing Aging Voting Systems, *Managing Election Technology Series #2”* [1] discusses the issue of aging voting systems. After the passage of HAVA, as the article mentions, there was a surge of voting system acquisitions across the country in the years 2002 to 2005. With rapid changes in technology, funding limitations, and increasing requirements about security, jurisdictions have to find ways to extend the life of some of these older systems. The EAC publication includes the following:

- Maintain a spreadsheet that includes the serial number for each voting system and ePollbook to record any issues with the equipment and the resolution.
- As you prepare for elections, run a stress test on the power supply and check all batteries that are used in the voting systems and their components.
- Watch for wear-and-tear of non-technical parts and repair or replace as necessary. Examples include Velcro strips, loose screws, and small washers and nuts.
- Monitor Technical Bulletins from your vendor for modifications, Engineering Change Orders (ECOs), end-of-life (EOL) components and related issues.
- Network with other election officials in the State using the same voting equipment.
- Evaluate your poll worker training materials after each election. Assess your poll workers’ learning.
- Conduct Logic & Accuracy testing of your voting systems before the required public test of voting systems. This pre-test will confirm if the voting system's tabulation matches the expected results from a pre-audited set of ballots. Any identified issues in the pre-test can be corrected before the public test.

Best Practices for Voting System Access: Both physical and cyber security are enhanced when an organization has well defined policies on who has access to the system. This includes both physical access to storage locations, and access to the systems and equipment. You must control and actively monitor access. The Belfer Center Report [5] includes several best practices for access control.

- Limit the number of people with access to the system to those who need it to complete their jobs (the “who”). [5] p.16
- Restrict what each user is authorized to do. [5] p.16
- Quickly remove those who no longer need access. [5] p.16

- Keep a list of all users who have access and their access levels.
- Regularly adjust access and permissions as personnel change. [5] p.19

Best Practices for Removable Media:

- Restrict the use of removable media devices (for example, USB/thumb drives, compact discs, memory cards) with voting systems. [5] p. 17
- Use only media that is approved/certified for use. Make sure you have back-up in the event of equipment failure. Know where to acquire/purchase removable media in the event yours becomes damaged.
- Limit the use of removable media only to voting systems.
- Scan media devices for malware. [5] p. 34
- When data on removable media is no longer needed, erase and reformat.
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy: “only use physical media once, from one system to a second system, then securely dispose of it.” [5] p. 20
- Keep an inventory and a chain of custody/tracking system for all removable media.

3. Best Practices for the Operation of Electronic Poll Books

Many of the best practices for voting systems also apply equally well to electronic poll books (ePBs). This section presents best practices for ePB operation. These best practices apply to all ePBs and are not vendor specific. We group the best practices into several categories.

Best Practices for Keeping your Electronic Poll Book Up-To-Date:

- Know the certification status of all your ePB equipment by consulting the VSTOP-ESI database or the IED/SOS website.
- Monitor technical bulletins from your vendor. Ask your vendor about any known or new issues.
- Ensure all devices are updated and patched. Test the electronic poll book to ensure that it is fully functional after patches have been applied.
- Monitor changes to your ePB such as modifications and engineering change orders. You may ask your vendor about any changes, contact VSTOP for the information or refer to the VSTOP-ESI inventory database.
- Follow your vendor's manuals and best practices for ePB operation.
- Keep a record of your ePB's maintenance.
- Follow your vendor’s guidelines for environmental requirements for storage and transportation of your ePBs and peripherals/accessories.

Best Practices for ePB Access: Both physical and cyber security are enhanced when an organization has well defined policies on who has access to the system. This includes both physical access, and access to the systems and equipment. You must control and actively monitor access. The Belfer Center Report [5] includes several best practices for access control.

- Limit the number of people with access to the [ePB] system to those who need it to complete their jobs (the “who”). [5] p.16
- Restrict what each user is authorized to do. [5] p.16
- Quickly remove those who no longer need access. [5] p.16

- Keep a list of all users who have access and their access levels.
- Regularly adjust access and permissions as personnel change. [5] p.19

Best Practices for ePB Operation:

- Make them single-purpose devices. [5] p.19 In other words, ePBs should not be used for any other purpose whether the ePB operates from a laptop or a tablet.
- Software on them should only be what is necessary. [5] p.19
- Understand how voter information is loaded onto the electronic poll books; confirm the electronic poll book file on the device matches the original file (Use hash codes if available). [5] p.19
- Ensure that the entire setup is preconfigured and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
- Ensure physical security. [5] p. 30
- Cover exposed ports (for example, USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. [5] p.30
- Do not use anything other than the original charging cord [5] p.30 (for example, do not use an iPhone charger or other similar charger that is not actually part of the ePB)
- Discuss with your vendor if your county needs the electronic poll book to be connected to your vendor's resources (like a server). If you do not need the [electronic poll book] to be connected to a vendor, SVRS, or the Internet while voting is taking place: turn off Bluetooth and wireless capabilities on the devices. It is better to disable these functions at the hardware level (for example, removing the wireless card) than to change a setting whenever possible. [5] p. 30
- Have a paper backup of the electronic poll book at each voting location. Alternatively, the county election board can print paper poll books on demand on election day to distribute to voting locations should a data breach or other connectivity issue occur.

4. **Elections Cybersecurity Best Practices**

- The Belfer Center, Harvard Kennedy School has published *The State and Local Election Cybersecurity Playbook* (See Section 7). This report includes several recommendations for establishing or improving cybersecurity for elections. The recommendations include:
  - Monitoring, logging, and backing up data. This enables attack detection and system or data recovery after an incident.
  - Backups should be regularly performed, either through automation or as part of a scheduled manual process.
  - Backups should be read-only once created to prevent data corruption.
  - Backups should be regularly tested by performing a complete restore from backed-up data.
- The National Institute of Standards and Technology (NIST) has published the *Framework for Improving Critical Infrastructure Cybersecurity 1.0* [4]. This report contains several recommendations for establishing or improving a cybersecurity program, which may also apply to cybersecurity for elections. Steps for improving such a program include:
  - Prioritize and Scope: Identify your high-level organizational priorities based on the most current cybersecurity threats to elections and election technology (VSTOP can assist counties in this area).

    - Orient: Identify related systems and assets.
    - Conduct a Risk Assessment (please see *Cybersecurity 1.0* above or consult with VSTOP).
    - Determine, Analyze, and Prioritize Gaps (based on the difference between current practices and Best Practices and anything identified in a risk assessment)
    - Implement Action Plan (VSTOP can assist with this. Additionally, a county election official in the CEATS program can develop such a plan as a capstone project).
- Be aware of recent changes in the State statutes (such as Indiana Senate Enrolled Act 327 - 2018) that relate to cybersecurity of voting equipment. See Section 6.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends
    - Securing networks and systems
        - Credential (e.g., usernames and passwords for logins) reuse policies
        - Use Two Factor Authentication (, a method whereby a user is required to enter more than a password, such as a code, to login to the system
    - Securing the End User (an "End User" is the ultimate consumer of hardware and software and in the instance of this manual would, in most cases, be an election official or poll worker)
    - Responding to a Compromise or Attack (Create a plan to respond to a compromise or attack on your election systems (ePBs or voting systems)
        - Detach the infected systems from the Network
        - Inform incident response team (IT Team) about attack
        - Run Anti-Virus and Anti-Malware on all systems to determine if other systems were infected
        - Delete all the infected files and restore the systems from the last backup before Infection.
    - Spear Phishing Tests (for an awareness of these attempts). Please see the glossary in this document for a definition of these types of campaigns.
- *The State and Local Election Cybersecurity Playbook* (See Section 7) also discusses Malware and its potential threat to voting equipment. One should treat all removable media as a potential delivery mechanism for malware. Some examples of Malware include the following.
    - Viruses – a type of malicious malware program that replicates itself, can corrupt and modify computer files, and can infect other systems
    - Trojan Horses – a malicious software program which entices a user to install it because it appears normal, routine or valuable for a system
    - Keyloggers – a covert method of computer keystroke recording whereby a malicious actor can log the keys used by a user to obtain valuable information such as usernames, passwords and other confidential information
    - Adware – a form of software that allows advertisements into a computer system and generates unwanted ads which may be of interest to a user
    - Spyware – a computer program which operates undetected in the background of a computer system in order to control a system or obtain information about the system and user without the user's knowledge
    - Worms – like viruses, worms can replicate themselves on a computer system using failures and limitations of the system's security in order to limit the system's capabilities
- If you need to connect an electronic poll book to external systems, there are certain security practices which should be followed. These include the following from *The State and Local Election Cybersecurity Playbook*:

  - Connect over a VPN (Virtual Private Network) or other encrypted channel. A VPN is a secure method of connectivity. [5] p.30
  - Ensure that the entire setup is preconfigured and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices). [5] p.30
  - Do not connect [electronic poll books] directly to the SVRS. Set up a separate system (essentially a copy of the SVRS) to handle changes to voter information, which prevents the SVRS from being impacted if an electronic poll book is compromised. [5] p.30
- The National Conference of State Legislators (NCSL) released the report *The Price of Democracy: Splitting the Bill for Elections* the day before on February 14, 2018 [6] which also includes suggestions and best practices for election security and cybersecurity. We also recommended a comprehensive review of this report. However, a few best practices pertaining to ePBs and VRDBs are noted here:
  - **Invest in cybersecurity personnel**. Hiring cybersecurity consultants or more IT staff may be useful. It can be helpful to work with outside experts, since they may be better prepared to find security holes than internal staff.
  - **Coordinate with others.** Sharing information within the state, between states, with federal agencies, and even between private entities can be the difference between discovering security holes and not. The Department of Homeland Security (DHS) offers cybersecurity assistance to election officials (see https://www.dhs.gov/topic/election-security), and there are organizations that help share security information between states as well, such as the Multi-State Information Sharing & Analysis Center (MS-ISAC). Some states have established partnerships with the National Guard to assist with protecting election systems from cyber threats. Private companies such as Google have also made commitments to providing assistance to state and local election officials (see: https://protectyourelection.withgoogle.com/intl/en/).
  - **Training.** Beefing up security can be as simple as providing training to state and local election officials on things like requiring strong passwords, activating existing security software that may be built into their systems, updating software as the vendor suggests, and teaching staff to avoid phishing and spear phishing efforts (please see the Glossary in this document for definitions of phishing and spear phishing). Overall, we must create a culture of security within election administration.
  - **Resiliency**. It's important for state and local officials to be able to monitor their systems, detect threats, respond, and then recover. What happens if the voter registration database is changed? Are there backups? Do state laws permit a "fail-safe" option for those who attempted to register but were thwarted by a cyberattack?
  - **Choosing secure equipment.** Security and resiliency of the systems can be a top-of-the-list priority. What is the backup in case of an attack on these systems?

5. **Elections Physical Security Best Practices**

- In a presentation at the 2018 Election Administrator's Conference, Beth Dlug, Director of Elections, Allen County, Jay Phelps, Clerk, Bartholomew County, and Laura Herzog, Elections Supervisor, Hendricks County described many excellent best practices for physical security. Below are some examples. See a copy of the presentation for the entire list.
  - Ensure that your voting system complies with VVSG.
  - Review VSTOP's certification and audit standards (Please see the EAC and SOS/IED websites or contact VSTOP).

  - Seal voting systems after public tests, which is required under IC 3-11-13-26 (optical scan systems) and IC 3-11-14.5-7 (DRE).
  - Deliver voting systems to the polling location no later than 6:00 pm the day before election, which is required under IC 3-11-13-6 and 3-11-14-14.
  - Record seal numbers, provide documentation of seal numbers in election materials for poll workers to compare against.
  - If numbers do not reconcile or seals are broken, inform county election officials immediately.
  - Secure the equipment after polls close.
  - Secure Absentee ballots under bipartisan lock-and-key until election day.
- Be aware of recent changes in state election code (such as Indiana Public Law 100 - 2018) that relate to physical security of voting equipment. See Section 6.
- Maintain an inventory of the voting systems and electronic poll books as required by IC 3-11-16-5 and provide this information to VSTOP. See Section 6.
- The report *Election Security: A Priority for Everyone*, published in NCSL's The Canvass, July 2017 [7] includes the following best practices:
  - Ballot reconciliation. Accounting for all ballots, those that were voted, spoiled in some way and set aside, or never voted.
  - Chain of custody. "Chain of custody" requirements come into play when there are any movements or actions relating to ballots, poll books, equipment and just about anything else. It's common practice to log everything, and to require bipartisan teams to work together in this process.
  - Secure physical storage. Between one election and the next, elections equipment has to be kept somewhere. Is that warehouse secured? Is there a log of who enters and exits? Are security cameras used? Are unmarked ballots secured too? While legislation on storage requirements is rare, it's a key issue with local or state officials. See the U.S. Election Assistance Commission's paper on 10 Things to Know About Managing Aging Voting Systems for more information as well as Indiana's Public Law 100 - 2018 for physical security provisions.
  - Contingency planning. Planning for crises and disasters. For instance, how would your county address a data breach to an ePollbook or loss of internet connectivity? What is your plan if a polling location cannot be used on Election Day due to an emergency? What happens if a power line is cut to a polling place on Election Day - can your voting systems work on battery back-up or do you have paper ballots that can be securely stored until power is restored? Are your poll workers trained?

6. Standards and Best Practices based on the Indiana Election Code

This section includes a description of recent Indiana election law that relates to the physical security and cybersecurity of elections and election equipment. Be aware of changes in state election code that relate to physical security of voting equipment. The following became effective March 15, 2018 or July 1, 2018 in some cases, pursuant to Public Law 100 - 2018. In future versions of this manual, additional Indiana Code will be referenced. It should be noted that election officials should be aware of already existing security provisions in the Indiana Election Code in addition to recent changes.

Indiana Code	Best Practice
IC 3-6-3.7-5: This permits a county election board to apply to the Secretary of State for reimbursement of expenditures made by the county to secure and monitor facilities where voting systems and electronic poll books are stored.	Keep track of the inventory/locations and expenses.
IC 3-11-7-20, IC 3-11-7.5-24, IC 3-11-8-10.3 (c): The county election board is responsible for the security of ballot card voting systems, direct record electronic voting systems, and electronic poll books when they are not in use.	Utilize the VSTOP-ESI database for tracking the inventory and locations. Please see communication from VSTOP regarding the web location for the database.
IC 3-11-13-22, IC 3-11-14.5-1: The public tests should include tests for correct counting of straight party votes and write-in votes.	Revise your tests to include this requirement, as needed. Ask VSTOP for IED approved tests for straight party counting.
IC 3-11-15-46: The county election board is responsible for access policies and security protocols. The VSTOP and IED shall be available to advise the county election board in the development of a security protocol under this subsection.	Discuss with VSTOP and IED to develop such protocols. Please refer to the sample packet provided to county clerks at the June 2018 SBoA conference in Indianapolis.
IC 3-11-15-59: The county election board must have a plan for disposal of election equipment.	Utilize the VSTOP-ESI database for tracking the inventory. Please see communication from VSTOP regarding the web location for the database. Inform VSTOP and IED when there are items ready for disposal and utilize the state form for IED approval of disposal.
IC 3-11-16-4, IC 3-11-16-5: VSTOP must maintain an inventory of voting systems and electronic poll books. Each county election board shall regularly provide information to the program to update the inventory of voting systems and electronic poll books	Use VSTOP-ESI training materials to maintain a current inventory of your election equipment. Please see communication from VSTOP regarding the web location for the database and the user manual in that location.
IC 3-11-17-7: The county election board must report improper access to election equipment or data.	Maintain proper chain-of-custody records. This can be maintained, for example, in spreadsheet form by a county official. The spreadsheet would need to include the date, the person accessing equipment, the equipment being accessed by serial or inventory number, the time the person entered the equipment room, the time the person exited the equipment room, and any other notes.

7. **Resources**

- **Federal and Other**
    - Election Assistance Commission and various versions of the Voluntary Voting System Guidelines (VVSG)
    - Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (NIST), February 12, 2014
    - U.S. Department of Homeland Security
    - Election Center
    - NIST – Framework for Improving Critical Infrastructure Cybersecurity 1.0, National Institute of Standards and Technology
    - Voting System and Electronic Poll Books Vendor documentation
    - NCSL.org National Council of State Legislatures - ELECTION SECURITY: STATE POLICIES
    - The State and Local Election Cybersecurity Playbook, Defending Digital Democracy Project, Belfer Center, Harvard Kennedy School
    - Election Cyber Incident Communications Plan Template for State and Local Officials, Belfer Center, Harvard Kennedy School
    - Hacking Chads - The Motivations, Threats, and Effects of Electoral Insecurity, Belfer Center, Harvard Kennedy School
- **State Level**
    - Indiana Department of Homeland Security - Election and Polling Place Emergency Preparedness Guide, October 22, 2012
    - Title 3 - Indiana Election Code
    - Indiana Election Division
    - Physical Security of Election Systems and Materials (Presentation by Beth Dlug et al. at the 2018 Election Administrator's Conference)

8. Glossary

The following Glossary of Information Technology and Election Administration terms is available at the U. S. Election Assistance Commission (EAC) website at https://www.eac.gov/documents/2017/09/21/information-technology-terminology-security/

General Information Technology

Access Controls Methods by which access to specific data, procedures, and other resources is restricted or controlled. The most common access control is a username/password combination. Two factor authentication (TFA) is highly recommended along with strong passwords made up of letters, numbers, and symbols.

Election officials must control access to resources within the scope of the election systems they supervise. A typical criteria is “need to know,” implying that election workers only have access to appropriate data and resources within the scope of their responsibility.

Accessibility Refers to the extent to which a site, facility, work environment, service, or program is easy to approach, enter, operate, participate in, and/or use safely and with dignity by a person with a disability.

Election officials must ensure that all aspects of the election are fully accessible to all voters.

Accountability Methods by which a system associates users and processes.

Election officials must be able to detect when an error occurs by logging the event. A main function of event logging is being able to determine who is accountable for the error.

Administrative Controls The policies and procedures implemented as part of its overall information security strategy.

Election officials must create an IT and security strategy that addresses the policies and procedures for securing their election systems.

Air Gap An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called “Sneaker Net.”

Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Algorithm A procedure or formula that produces predictable, consistent results when applied. An algorithm describes, in formal language (frequently mathematical) how a problem is solved. An algorithm, like a recipe, is a well prescribed sequence of steps designed to produce a solution.

The procedure that produces a uniform distribution of ordered candidates within a race in a ballot rotation scheme is an algorithm. Counting votes in an instant runoff voting system requires a specific algorithm.

Application Programming Interface (API) Specification for input data and output data for a system.

Election officials can use APIs to adapt their election systems for commonly used applications, such as the Voter Information Project (VIP) for voter lookup tools and election night reporting

Assistive Technology A device that improves or maintains the capabilities of people with disabilities (no vision, low vision, mobility, cognitive, etc.).
Assistive technologies include headsets, keypads, software, sip-and-puff, and voice synthesizers.

Accessibility of voting systems in accomplished through good, universal design principles and assistive technologies.

Audit A review of a system and its controls to determine its operational status and the accuracy of its outputs.

Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Backdoor An undocumented or hidden entry into a computer system that permits unauthorized access to programs and/or data. Some early voting systems had backdoors that permitted developers to access system functionality without logins.

Bandwidth The throughput capacity of digital connections. Large data files (like an electors list) require significant bandwidth capacity to move through a network. Low bandwidth means slow connection speeds.

Barcode A barcode is an optical, machine-readable representation of data relating to an object. Barcodes come in a variety of formats including 1D (barcode 39 or 128) and 2D (pdf 417). Barcodes can also be encrypted. Barcoding is a common technique to permit rapid identification of ballots, election materials, and voter records.

Blacklist A list of URLs, domains, users, or other identifiers, that have system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Blockchain A database that holds a continuously growing set of encrypted transactions, in a tamper proof format. Blockchain is the underlying architecture for Bitcoin technology. Online voting systems have been proposed that use Blockchain architecture.

Boolean Pertaining to one of two states: off/on, 1/0, Yes/No, or some other binary pairing. When a voting system is tested, most of the tests are Boolean in nature – that is, the system completely passes or completely fails the test.

Botnet A programmed Internet connected device that can be used to launch DDOS attacks, steal data, send spam, etc. Bots are frequently spread as email attachments and can compromise election office computers used to browse websites and support email activities.

Browser Software program installed on a computer, that permits the user to access the Internet, download files, print files, and perform other operations. Common browsers are Microsoft's Internet Explorer, Mozilla's Firefox, and Apple's Safari. Not all applications will run on every browser. Election Night Reporting Systems, voter information pages, and other Internet applications may appear different, in different browsers. Check systems for browser compatibility.

Byte Eight binary digits or the amount of data used to store a character or an integer – a measurement of storage in a computer's memory or its storage media. The average voter record consists of about 200 characters. That would require 200 bytes of storage, plus some storage for meta data. To store 6 million voter records on a memory card, that card needs to have at least 1.2 Giga Bytes of memory.

Ciphertext Data or information in its encrypted form. Election data will display in cyphertext – and be unreadable by humans – without decryption.

Cloud Computing The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Also called on-line computing.

Election technologies are evolving in parallel with other commercial information systems. Election officials may be managing voter and election data, stored on computers, outside of their organization. Cloud computing requires an appropriate security strategy to ensure the protection, availability and integrity of data and programs store in the cloud.

Code n. Synonym for program or software. v. to create or modify software.

Commercial Off-The-Shelf Technology (COTS) Hardware and software components that are widely available for purchase and can be integrated into special-purpose systems.

E-pollbooks are often implemented on COTS tablets such as the iPad or Android tablet. COTS systems are contrasted with propriety systems.

Common Data Format Standard and practice of storing and creating data in a common, described format that can be read by other systems.

Voting and election systems that use a common data format can share data without middleware software to convert it. Election Night Reporting systems are common applications that anticipate a common data format for input.

Controls A device, procedure, or subsystem, which when properly designed and implemented, ensures correctness of operation in a system. Common controls include completeness of processing checks, authentication of users, and accuracy in processing. Controls can be preventative (prevent anomalies from occurring) or paired, detective and corrective controls.

A common detective control in election administration is a physical seal. The seal does not prevent tampering with election devices but permits the detection of tampering.

Custodian Person with the responsibility for protecting information assets.

IT personnel or an IT Division may be the custodian of voter registration systems and other systems that are maintained in house. For a precinct-based voting system, the custodian may be an election worker who is in charge verifying seals and making sure no unauthorized access is gained to the voting devices.

Cybersecurity Measures taken to protect computer systems from attack and unauthorized access or use. Cybersecurity tools include hardware, software and procedures.

Election officials must defend against attacks and unauthorized access of election and voting systems. The most common cybersecurity technique is good password management.

Data destruction The removal of data from a storage medium.

Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database A structured collection of data that includes data and meta data (data about the data). Databases are managed by Database Management Systems.

The election database stores all of the requisite information to manage election including precinct information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Defense-in-Depth Also called the “Castle” approach. Multiple levels of logical and physical security measures that deny a single point of security failure in a system.

The use of passwords, encryption, lock-and-key access, security seals, and logs, represents a defense-in-depth approach to securing voting and election systems.

Digital Certificate A technology by which systems and their users can employ the security applications of Public Key Infrastructure (PKI). PKI is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Voting and election systems will use PKI infrastructure to exchange and compare digital certificates for the purpose of authenticating access and securing transmission of data.

Digitize To convert analog data to digital format for storage and use on a computer. The digital form of the character “A” is the byte: 01000001 (ASCII value 65). Any data stored in a computer must be digitized. Converting the information on the front of a voter ID card or driver’s license into a computer readable format requires the data to be digitized. Scanners are digitizers.

Directory A file storage architecture in which individual files are stored in separate, hierarchical directories. The directory is the map to where the file is stored. Most systems will store files in a default directory unless otherwise specified.

Election systems will store files in directories on both internal and external storage media. Finding a file requires the election official to know not only the file name, but also the directory name in which the file is stored.

Domain A collection of users, computers, and resources that have a common security policy administered by a single entity.

Download Transferring data from a larger computer to a smaller computer or device.

An EMS facilitates downloading ballot images to vote capture devices.

Dox Publish damaging or defamatory information about an individual or organization on the Internet.

One method of hacking a campaign is doxing (or doxxing).

Dynamic password A password that changes at a defined interval or event.

Entitlement Access rights assigned to employees based on job title, department, or other established criteria.

Ethernet A network protocol (IEEE 802.n) that is used to permit local area network devices to communicate with each other. Ethernet connections use a Cat 5e connector cable.

Many of the devices used in polling places will use an Ethernet connection to establish connectivity with other devices (e-pollbooks, card activators, etc.).

Encryption The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it.
Encryption does not prevent interception but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down.

Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

End of Life (EOL) When the manufacturer or integrator of an IT component ceases to produce and provide technical support for that product.

Election officials who use technologies that are EOL'd, should monitor available inventories and begin to create a transition strategy to newer, supportable technology.

Escalation of privilege An attack where the attacker is using some means to bypass security controls in order to attain a higher privilege level on the target system.

Exfiltration – Unauthorized transfer of information from an information system.

A data breach of an election system may lead to the exfiltration of PII data.

Failover A mode where the system automatically transfers processing to a backup component when a hardware or software failure is detected.

Fail-safe A mode where program execution is terminated to protect the system from being compromised when a hardware or software failure is detected.

Fail-soft A mode where non-critical processing is terminated to protect the system from being compromised when a hardware or software failure is detected.

Failure The inability of a system or component to perform its required functions within specified performance requirements.

Fault Momentary loss of electrical power.

Fault-Tolerant A system that continues to operate after the failure of a computer or network component.

File A collection of related data, stored on media. Files will be identified by a system-valid filename.

File type – The specific kind of information contained in a file, usually designated with a file extension (for example, .doc for a Word document; .txt for a text document, etc.). A .pdf file is common format for reports (See **Portable Document Format)**

Systems will usually expect a specific file type for input/output operations. Your election night reporting system may accept only a .txt file or a .zip file.

FIPS (Federal Information Processing Standards) Standards issued by US Government for use in government agencies. FIPS 140 covers encryption standards.

Firewall A gateway computer and its software that protects a network by filtering the traffic that passes through it.

Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the internet.

Firmware Computer instructions that are encoded directly into computer hardware. Firmware is resident to the hardware and cannot be altered without modifying the hardware.

Voting systems may contain firmware that cannot be altered without replacing the hardware.

FTP (File Transfer Protocol) A standard network protocol used to transfer computer files between a client and server on a computer network, usually the Internet.

Election offices will upload and download files, such as sample ballots or election databases, using an

FTP site. FTP requires the use of password authentication.

Gateway A system, connected to a network, which performs real-time translation or interface function.

Glitch An intermittent system error of undetermined cause. A system glitch may cause a network to go offline or a program to crash.

Election officials are expected to track down all errors to their root causes and avoid blaming anomalies on "glitches."

Hacker Someone who seeks to exploit weaknesses in computer systems, voting systems or networks to gain unauthorized access or break-in into a system. There are many types of hackers, but the best-defined terms for types of hackers are white-hat and black-hat hackers

Hacking The act performed by a hacker whereby the hacker gains unauthorized access or breaks-in into a system by exploiting a weakness.

Hacktivism Utilizing technology to publicize a social, ideological, religious or political message.

Hacktivism can refer to any attempt to alter or influence the outcome of an election by an interested third party, such as a nation state. It can also refer making information that is not public, or is public in non-machine-readable formats, accessible to the public

Hardware The physical, tangible, mechanical or electromechanical components of a system. If you can put an inventory sticker on it – it's hardware.

Voting system hardware must be physically secured with locks, seals, and logs. Hardware may be COTS or proprietary. Proprietary hardware is unique to the vendor and purchase, maintenance and repairs will be done by the voting system vendor. Hardware can be repurposed by upgrading the software that controls it.

Hash Function A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes

Voting system object code is "hashed" so that installations can be validated as identical to the certified version.

Heterogeneous environment An environment consisting of multiple types of systems.

Homogeneous environment An environment consisting of a single type of system.

Hub A network device used to connect several LAN devices together.

Hypertext Transfer Protocol (HTTP) An application protocol to transfer data between web servers and web browsers.

Hypertext Transfer Protocol Secure (HTTPS) The HTTP protocol encrypted with SSL or TLS.

Inactivity timeout A mechanism that locks, suspends, or logs off a user after a specified period of inactivity.

Interface A boundary between two components of a system**,** through which the components may interacts or share information.

Examples: A hardware interface connects input/output devices. Humans and computers interact though user interfaces.

A DRE presents an interface to the voter. This interface permits the voter to interact with the system via a touchscreen, wheel, or some other input device.

Internet Global, public network that permits computers and other devices to be interconnected.

Election offices may have desktop, laptops, tables and other computers connected to the Internet so that information can be uploaded and downloaded and applications like email can be run. Once a device is connected to the Internet it is potentially accessible by anyone, from anywhere. Internet access carries with it certain security risks.

Internet Service Provider (ISP) Organization that provides access to the Internet for customers or members.

Examples include AT&T, Comcast, etc.

Interoperability The extent to which systems and devices can communicate with each other and work cooperatively without extensive modification by a systems integrator or programmer.

The extent to which you can change out components of a system is a measure of the interoperability of that system. Generally speaking, interoperability permits an election official a wider range of options for maintenance and support of their voting system.

Intranet A local network of computers and other devices that moves and stores information within the organization.

Election offices may use an intranet to store election related data that is not accessible from outside of the office.

Intrusion detection system (IDS) A hardware or software application that detects and reports a suspected security breach, policy violation or other compromise that may adversely affect the network.

Intrusion prevention system (IPS) A hardware or software application that detects and blocks a suspected security breach, policy violation or other compromise that may adversely affect the network.

IP Address Internet Protocol Address. An IP Address is numeric value (nnn.nnn.nn.nn) used to uniquely identify a device within a network. The address can also be used for local networks.

Many devices in an election office may be linked together on a local network that utilized IP addressed to identify devices. Accurate settings of the IP address are critical to permit devices to communicate with each other.

Java applet A software application written in the Java programming language that is usually launched through a web page. Browsers must be configured to interpret Java applets.

ENRs and Voter Information Pages often include Java applets.

Local Area Network (LAN). Also see MAN and WAN. A computer network that connects computer and other devices such as printers in a limited area such as a school, office building or home.

Computers and devices in an Election Management Center may be connected with a LAN.

Life Cycle Systems engineering concept that identifies the phases that a system passes through, from concept to retirement. There are different concerns and activities associated with each phase of the life cycle.

The adoption, deployment, use and maintenance of voting and election systems require different life cycle concerns and activities, depending upon where in the life cycle the system resides.

Malware Various types of malicious software intentionally designed to cause damage to a computer, server or computer network.

Message digest A condensed representation of a message that is produced by using a one-way hash function.

Multi-factor authentication Authentication mechanism requiring two or more of the following: something you know (for example, Password), something you have (for example, Token), something you are (for example, biometrics).

National Institute of Standards and Technology (NIST) Federal organization tasked with assisting in the development of voting system standards (see VVSG). NIST develops and maintains standards for a wide array of technologies.

NIST scientists assist the EAC in developing testable standards for voting systems.

Open Source Computer software with its source code (human readable code) made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open source software may be developed in a collaborative public manner.

Voting and election systems that contain open source software have had that software reviewed by multiple, professional and amateur programmers.
Open source systems are usually not free and are typically licensed like other software. Systems can be fully open source, or may have only a portion of their software open source.

Operating System A collection of programs that controls the hardware of a computer system and provides utilities and services to application software that is installed on the device. Operating systems use complex release version numbers to indicate which version is installed and require frequent patches or updates to maintain security and functionality.

Managing the software revisions in an election office requires careful coordination of updates to the operating system as well as to the application software.

Owner An individual responsible for management of an asset and its policies.

Penetration Testing Also called Pen Testing. An evaluation method that enables researcher to search for vulnerabilities in a system.

Election systems, such as the VR system, are periodically submitted to Pen Test to determine their vulnerabilities to cyber-attacks.

Phishing A general attack by hackers, via bogus emails, that attempts to get victims to provide login information or personal information to the hackers. Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors.

Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

PII Personal Identifying Information. Information that permits the identity of an individual to be derived and possibly used for identity theft.
Voter registration systems may contain PII.

Portable Document Format (pdf) A standard and commonly used file format, used for creating, sharing, and reading documents, forms, and reports. Pdf files can only be opened and read by a reader, such as Adobe Acrobat.

A lab report for a voting system and a form for voter registrations are common examples of pdf files.

Preventive controls Controls that prevent unwanted events.

Program *n.* A set of instructions that are stored within a computer's memory and cause the computer to execute a task. *v.* The process of creating a computer program.

Election databases are programmed to store all the data as well as the rules of processing that data, for a given election. Ballot builders are sometimes referred to as election database programmers.

Protocol 1. An agreed upon format for transmitting data between devices. 2. A plan for carrying out a formal or scientific study.

Voting system tests are often called protocols.

Proxy server A system that transfers data packets from one network to another.

QR Code Quick Response Code. A 2-D, trademarked bar code.

Some proprietary voting systems will encode the voter's choices in a QR Code that can be read on a scanner in the precinct and converted to a printed ballot.

Ransomware Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device.

Election office computers should maintain high levels of cyber hygiene, including up-to-date anti-malware systems and adherence to best practices regarding managing browser and email client activities.

Requirements The fundamental collection of activities and functions that must be supported by a system. Defining requirements determines the capabilities of the system.

Election officials must be able to articulate the fundamental set of things a voting system or election system must do, in order to define the requirements of the system. These requirements are then reiterated in Request for Proposals (RFPs) and subsequent contracts with vendors.

Router A device that manages network traffic by passing data packets between different networks.

A wireless router may be used to permit EPBs to communicate with each other at a precinct or vote center.

Server A server is a collection of computer programs, hosted on a computer that provides services to other computers, via some connection – usually a network.

Voting systems use special-purpose servers to create closed networks for uploading and downloading information from voting system media (memory cards). These servers also contain the tabulation software.

Social Engineering Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech.

Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer.

The Election Management System (EMS) used to create election databases is software.

Source Code Human readable computer instructions that when compiled or interpreted, become an application. Source code can be written by humans or by computers. The source code of a voting system must be securely stored (escrowed) so that any future, needed modifications of the system can be performed.

Spear Phishing A targeted attack by hackers (toward a particular person or entity), via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors.

Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Switch Switches connects computers in a network. A switch acts as a controller. Thus, switches create networks. Routers connect and manage traffic between different networks.

One or more DREs might be connected via a switch to the EMS.

System A collection of unified components that convert inputs to outputs. Systems consist of integrated subsystems. Systems are typically complex and highly interconnected. Information systems consist of hardware, software, data, people and procedures.

The voting system is more than just a single device. It consists of numerous subsystems, which when unified and controlled, give the voting system its capabilities. Subsystems include vote capture, vote tabulation, reporting, etc.

Software Patches Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes.

Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning.

Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Uninterruptable Power Supply (UPS) A battery powered back-up system that quickly switches to battery power when electrical current to the computer system is disrupted (surge, sags, and failures). Election offices ensure election operations continuity by utilizing UPS systems in the event of a power failure. UPS systems come in various sizes and are rated by hours/minutes of service following a power failure.

Upload Transfer data from a smaller computer or device to a larger computer.

At the close of polls, memory cards with cast ballot information are uploaded to the central tabulation computer.

Virtual Provide Network (VPN) A VPN is a secure method of computer system connectivity.

Virus A malicious computer program that may replicate itself on in a computer network, insert or attach copies of itself into computer programs, and cause harm to computers or systems by corrupting, stealing or modifying data or access.

Voting system components connected to a network risk malware infections, such as viruses.

Wi-Fi Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections.

Some e-pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Wide Area Network (WAN) A network that connects computers across metropolitan, regional and national boundaries.

The internet is an example of a WAN.

Wireless Network connectivity using radio waves instead of wire connections. Wireless signals can be intercepted and, if not encrypted, deciphered.

Election systems that use wireless connectivity must be tested for security and signal reliability.

XML Extensible Markup Language XML is a text-based language used to organize and present information on the World Wide Web. Some Election Night Reporting (ENR) systems use XML coding for their displays. The voting system must be able to export reports in (or convert them to) XML format.

Election Administration Technology

Acceptance Testing Testing each individual unit of the voting system for conformance to the certified model. Acceptance testing should not be done by the vendor and should be done any time the voting system unit falls out of custody of the jurisdiction. In Indiana electronic poll books also undergo acceptance testing.

Automatic Voter Registration (AVR) Voter registration subsystem that creates a voter record automatically from an external (usually DMV) transaction. AVR systems require a voter to “opt out” if they choose not to be registered (It should be noted that Indiana does not have automatic voter registration. However, Indiana does have “motor voter”).

Ballot On Demand (BOD) Ballot On Demand systems permit a jurisdiction to print paper, optical scan ballots as needed. BOD systems integrate ballot images from the EMS and data from the voter registration system to select the correct image for printing. In theory BOD systems prevent over ordering of ballots and ensure that the jurisdiction does not run out of ballots during the election.

Barcode Reader Device used to scan barcodes and convert the encoded information into a usable format. Barcode readers are used to scan codes on ballots, driver’s licenses, voter ID cards, voter information packets, envelopes, and other documents in the election ecosphere.

Central Count Optical Scan Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies.

Digital Optical Scan System Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems. Often these systems have an electronic interface for a voter to mark their candidate selections digitally and an optical scan paper ballot card is printed with their selections. The ballot card is then inserted into the optical scan component of the system where the results are tabulated.

Direct Record Electronic Voting System (DRE) A DRE system presents a ballot image to a voter, collects the voter’s choices, and records those choices directly onto electronic media. DREs may be fitted with Voter-verifiable paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction, image displays, and can hold a large number of ballot styles in multiple languages.

Election Management System (EMS) The collection of software systems that are used by election officials to "build ballots." The EMS defines ballots by associating precincts with races and candidates and describing how those ballot components will be displayed. The EMS is also responsible for tabulation, report generation and auditing.

Election Night Reporting Systems (ENR) A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Ballot Delivery The delivery of ballot and voter information packets via the Internet. The Military & Overseas Voter Empowerment Act (MOVE) requires each state to provide for the electronic delivery of ballots and related information from the local election office to the registered voter covered by the Uniformed & Overseas Citizens Absentee Voting Act (UOCAVA).

Electronic Ballot Return The return of a voted ballot or voter information packet via electronic means. This can be by fax, email, or through the use of an Internet supported application. Sometimes referred to as "Internet Voting."

Electronic Poll Book (EPB) Hardware and/or software that permits election officials to review the list of registered voters and mark voters who have been issued a ballot. Also called e-pollbook. E-pollbooks can be stand alone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

Geographical Information System (GIS) A system designed to capture, store, manipulate, analyze, manage, and present all types of spatial or geographical data. GIS systems are used to validate voting district boundaries and may be integrated with the voter registration system.

High Speed Central Count Tabulation System An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Logic and Accuracy (L&A) Testing Several jurisdictions around the United States are required to test the correctness of every ballot style and to determine that every possible valid and invalid voter choice can be captured or handled by the voting system, both technologically and legally. L&A scripts are developed to test both the ballot and the vote capture and tabulation systems.

Indiana Jurisdictions are not required to do L&A testing; instead, they are required to conduct a public test. Before the public test of voting systems, county election administrators are strongly encouraged to perform L&A testing. This is a pre-test of the voting system using an audited deck of ballots with a pre-determined outcome to ensure all candidates receive a vote, and in a November election the straight party option is also tested. Further, the test deck must test for an over-vote for counties using an optical scan system and an under-vote in counties using an optical scan system or DRE. L&A testing ensures any issues with system coding can be corrected before the legally required public test of voting systems.

Online Voter Registration (OVR) Voter registration subsystem that permits individual users to remotely create, edit or review their own voter record within the voter registration system.

However, in Indiana voters do not create or edit their record within the system. A person may submit an application to register to vote or update an existing registration, though the changes are not automatic and require county validation and the mailing of a voter acknowledgment card.

Optical Scan System (Op Scan) A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan Optical scan technology that permits voters to mark their ballot cards within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Remote Ballot Marking Devices Remote ballot marking systems are used in some jurisdictions nationwide, which assist military and overseas voters in completing their ballot. These allow a voter to obtain an official ballot which is blank that can then be marked electronically, printed, and returned to an elections office as a ballot to be cast in an election.

Risk Limiting Audit Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Technical Data Package (TDP) A collection of documents that describe a voting system, including manuals, a description of components and details of architectural and engineering design.

Voluntary Voting System Guidelines (VVSG) Collection of standards that is developed and maintained by the U.S. Election Assistance Commission (EAC). The VVSG specifies a minimum set of performance requirements that voting systems must demonstrate when tested by the VSTLs. Please see https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

Vote By Mail (VBM) Method of casting ballots by which eligible voters are mailed ballots and information packets by the local jurisdiction. Voters can return their marked ballots by mail or drop them off in secure drop boxes. Vote By Mail replaces Election Day voting at polling locations, and should not be confused with Indiana's absentee-by-mail option.

Voter Registration System (VRS) A distributed or centralized system that permits the collection, storage, editing, deletion and reporting of voter records. HAVA requires each state to have a centralized, statewide voter registration system (VRS). A VRS has multiple interfaces and can interact with Department of Motor Vehicle (DMV) systems, election officials, voters and other stakeholders. The VRS may be vendor-provided or “homegrown.”

Voting System The total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information.

Voting System Test Labs (VSTLs) VSTLs are privately owned testing laboratories that test voting systems (and other election systems) for conformance to the Voluntary Voting System Guidelines (VVSG) or to other requirements, including individual state requirements. VSTLs are periodically reviewed for conformance to National Voluntary Laboratory Accreditation Program (NVLAP) administered by the National Institute for Standards and Technology (NIST). In 2016, there were three accredited VSTLs.

Voter Verified Paper Audit Trail (VVPAT) Contemporaneous (or real-time) paper-based printout of voter choices on a DRE.

End Notes

1. Ten Things to Know About Selecting a Voting System, Managing Election Technology Series #1, United States Election Assistance Commission https://www.eac.gov/assets/1/28/Managing%20Election%20Technology%20Series%201%20Ten%20Things%20FINAL.6.24.15.pdf
2. "Indiana Electronic Poll Book (ePollBook) Certification Test Protocol," http://www.in.gov/sos/elections/files/doc00354920170908122519.pdf
3. 10 Things to Know About Managing Aging Voting Systems, *Managing Election Technology Series #2*, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-managing-aging-voting-systems-voting-technology-voting-systems-cybersecurity/
4. Framework for Improving Critical Infrastructure Cybersecurity 1.0, National Institute of Standards and Technology, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
5. The State and Local Election Cybersecurity Playbook by Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#securing
6. The Price of Democracy: Splitting the Bill for Elections by the National Conference of State Legislators (NCSL), http://www.ncsl.org/research/elections-and-campaigns/the-price-of-democracy-splitting-the-bill-for-elections.aspx
7. Election Security: A priority for everyone by the National Conference of State Legislators (NCSL), http://www.ncsl.org/research/elections-and-campaigns/states-and-election-reform-the-canvass-july-2017.aspx#Election%20Security

Voting System Technical Oversight Program at Ball State University (VSTOP)

Risk Limiting Audit (RLA) Pilot

May 2018

Post-Election Risk Limiting Audit Pilot

Marion County Indiana

May 30, 2018

An Introduction

A Collaboration between Marion County Office of the Clerk, Office of the Indiana Secretary of State, Indiana Governor's Executive Council on Cybersecurity, U.S. Election Assistance Commission, Caltech/MIT Voting Technology Project, and the Voting System Technical Oversight Program (VSTOP)

VSTOP

Indianapolis

U.S. Election
Assistance
Commission

Indiana
Secretary
of State

Caltech/MIT
Voting Technology Project

Introduction

In January 2017, U.S. Elections Systems were designated as part of the nation's critical infrastructure by the United States Department of Homeland Security. Also, in January 2017, Indiana Governor Holcomb signed an Executive Order to continue the Indiana Executive Council on Cybersecurity (IECC) (https://www.in.gov/cybersecurity/2570.htm). The Executive Council comprises ten committees and several working groups. The Elections Committee of the Council is chaired by the Indiana Secretary of State Hon. Connie Lawson. Dr. Jay Bagga of the Voting System Technical Oversight Program (VSTOP) serves as an Advisory Member to this Council and is a member of the Elections Committee.

One of the deliverables for the Elections Committee is to create a **Post-election risk limiting audit (RLA)** protocol proposal. As a component of this activity, VSTOP proposed conducting a pilot RLA in some Indiana counties. VSTOP began discussing the RLA process with Jerome Lovato, Election Technology Specialist at the U. S. Election Assistance Commission.

VSTOP considered several counties for such an audit. It is important to note that only jurisdictions with Voter Verifiable Paper Ballots are amenable to RLAs. VSTOP selected Marion County for this and a variety of other reasons, including its high voter registration. With the approval of Secretary Lawson and the Co-Directors of the Indiana Election Division, VSTOP held discussions with Marion County Elections Officials to discuss a potential partnership. VSTOP was pleased that in April 2018 Marion County agreed to be our partner for this endeavor.

The RLA Pilot will be conducted in Marion County, Indianapolis on May 30, 2018. In planning for this audit, Mr. Lovato proposed that the RLA Pilot include methods proposed by Dr. Philip B. Stark (Berkeley) and Dr. Ronald L. Rivest (MIT). These methods, the RLA method and the Bayesian Method will be used in the pilot for several races from the 2016 and 2018 elections. The races we are planning to audit are the Presidential Race from the November 2016 General Election, the U.S. Senate Race from the November 2018 Republican Primary Election, and the Sheriff Race from the 2018 Democratic Primary Election.

Marion County uses the ES&S EVS 5.2.2.0 which is an OpScan Voting System. This voting system is used in five other Indiana counties. The experience gained from a successful pilot audit can serve as the basis for RLA replication in other counties.

The RLA Pilot Team has relied on many of the lessons learned from the State of Colorado which was the first state to mandate Risk Limiting Audits as part of their post-election audit procedures. At this time not all Counties in Indiana have the capability to conduct a Post-Election Audit because we are not aware of any Direct Recording Electronic (DRE) Voting machines certified in the state of Indiana that produce a voter-verifiable paper audit trail.

VSTOP, Mr. Lovato, Dr. Rivest, as well as members of Marion County Elections Officials have held weekly WebEx planning meetings since the beginning of May. The RLA Pilot Team will meet at the Marion County Election Service Center on the afternoon of May 29th to organize and prepare for the Audits to be held on May 30th.

Based on a process assessment and the outcome of this initial Post-Election Audit initiative, VSTOP will advise the Indiana Secretary of State and the Governor's Indiana Executive Council on Cybersecurity regarding the future potential uses of post-election audits within the state of Indiana.

A Brief Overview of Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology. There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally there are two types of statistical methods: RLA and Bayesian.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Coordinated elections are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California secretary of state recently completed a three-year pilot program that audited contests of varying size in counties throughout the state.

In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

References

- A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
- A Bayesian Method for Auditing Elections https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

For more details please see the PowerPoint presentation by Jerome Lovato at the end of this document. This PowerPoint may differ slightly from the final presentation provided on May 30th.

Marion County Post-Election Audit Pilot Agenda

Location: Election Service Center at 3737 E. Washington St., Indianapolis, IN 46201

Day 1 – May 29th 12:00 PM – 4:30PM

12:00 PM	VSTOP: Introductions
12:15 PM	County: Review state/county guidelines for handling ballots and accessing restricted areas
12:30 PM	County: Walk through procedure for organizing and storing ballots
1:00 PM	J. Lovato: Provide Risk Limiting Audit (RLA) overview to county officials (Q&A)
1:30 PM	Create/Review Ballot Manifests, organize ballots for audits
3:00 PM	Ensure Primary ballots are separated by Democratic and Republican categories, nonpartisan, if applicable
4:00 PM	Phone Conference with Secretary Lawson

Day 2 – May 30th 8:30 AM – 3:30 PM

8:30 AM	VSTOP: Introductions J. Lovato: Risk Limiting Audit overview Dr. Rivest: Bayesian Audit Method
9:15 AM	Ballot Polling Audit of 2016 Presidential Race in Precincts LA-02, WS-49, PE-39, WR-23 and WS-69
10:00 AM	Break
10:15 AM	Ballot Polling Audit of 2018 Republican U.S. Senate Race in Precincts TBD
11:00 AM	Ballot Polling Audit of 2018 Democrat Marion County Sheriff in Precincts TBD
Noon	Remarks by Secretary Connie Lawson
12:15 PM	Lunch Break
1:30 PM	Bayesian Audit of 2016 Presidential, 2018 Primary R-U.S. Senate Race 2018 Primary D-Sheriff Race
2:15 PM	J. Lovato: Example/demo of comparison audit procedures
3:00 PM	Conclusion

The RLA Pilot Team

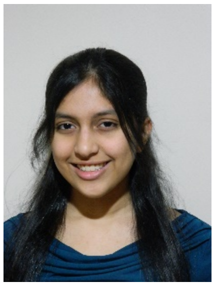
Jerome Lovato, Election Technology Specialist, U. S. Election Assistance Commission (EAC)

Jerome received his Bachelor of Science in Electrical Engineering from the University of Colorado at Denver. After working as an electrical engineer in the consumer electronics industry for six years, he worked as a Voting Systems Specialist at the Colorado Secretary of State's office for 10 years as a Voting System Certification Lead and Risk-Limiting Audit Project manager. Currently, he is an Election Technology Specialist for the U.S. Election Assistance Commission. Jerome led the team in Colorado that employed the RLA method. The following link is a gentle introduction to this method: https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Dr. Ronald L. Rivest, Institute Professor at MIT

Professor Rivest is an Institute Professor at MIT. He joined MIT in 1974 as a faculty member in the Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. He is a co-author (with Cormen, Leiserson, and Stein) of the text, *Introduction to Algorithms*. He is also a founder of RSA Data Security, now named RSA Security (the security division of EMC), Versign, and Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, electronic voting, and algorithms. A paper on the Bayesian method can be found at: https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

Mayuri Sridhar, Research and Innovation Scholar, MIT



Mayuri Sridhar is a Master's student studying Artificial Intelligence at MIT. She completed her undergraduate degree at MIT, double majoring in computer science and mathematics. Her research, under Profesor Rivest's supervision, focuses on statistics and optimization, applied to election audits.

Marion County Clerk's Office

Myla A. Eldridge, County Clerk
Brienne Delaney, Director of Elections
Jenny Troutman, Deputy Director of Elections
Joanna Alexander, Absentee Administrator
Colin Claycomb, Ballot Administrator
Rhonda Hawkins, Service Center Manager
and other county staff personnel

The VSTOP Team

Dr. Jay Bagga and Dr. Bryan Byers, VSTOP Co-Directors
Jessica Martin, VSTOP Project Manager
Mani Kilaru, VSTOP IT Specialist
Molly Owens, VSTOP Graduate Assistant
Contact: VSTOP@bsu.edu

Statistical Post-Election Audit Pilot

at Marion County, IN

Jerome Lovato, Election Technology Specialist

U.S. Election Assistance Commission

Goals

We will conduct a ballot-polling risk-limiting audit (RLA) and Bayesian audit. If time allows, we will also a conduct a comparison RLA.

The data gathered from this pilot will be used by the Voting System Technical Oversight Program (VSTOP) to assist in their development of a post-election audit protocol proposal for Indiana, and will be used by other jurisdictions throughout the U.S. that are considering conducting post-election audits using these methods.

Statistical Audit Methods - Terminology

A risk-limiting audit provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.[1] There are two main types of RLAs: ballot-polling and comparison.

The risk limit is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome.

A Bayesian audit is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else finds out the correct contest outcome.[2]

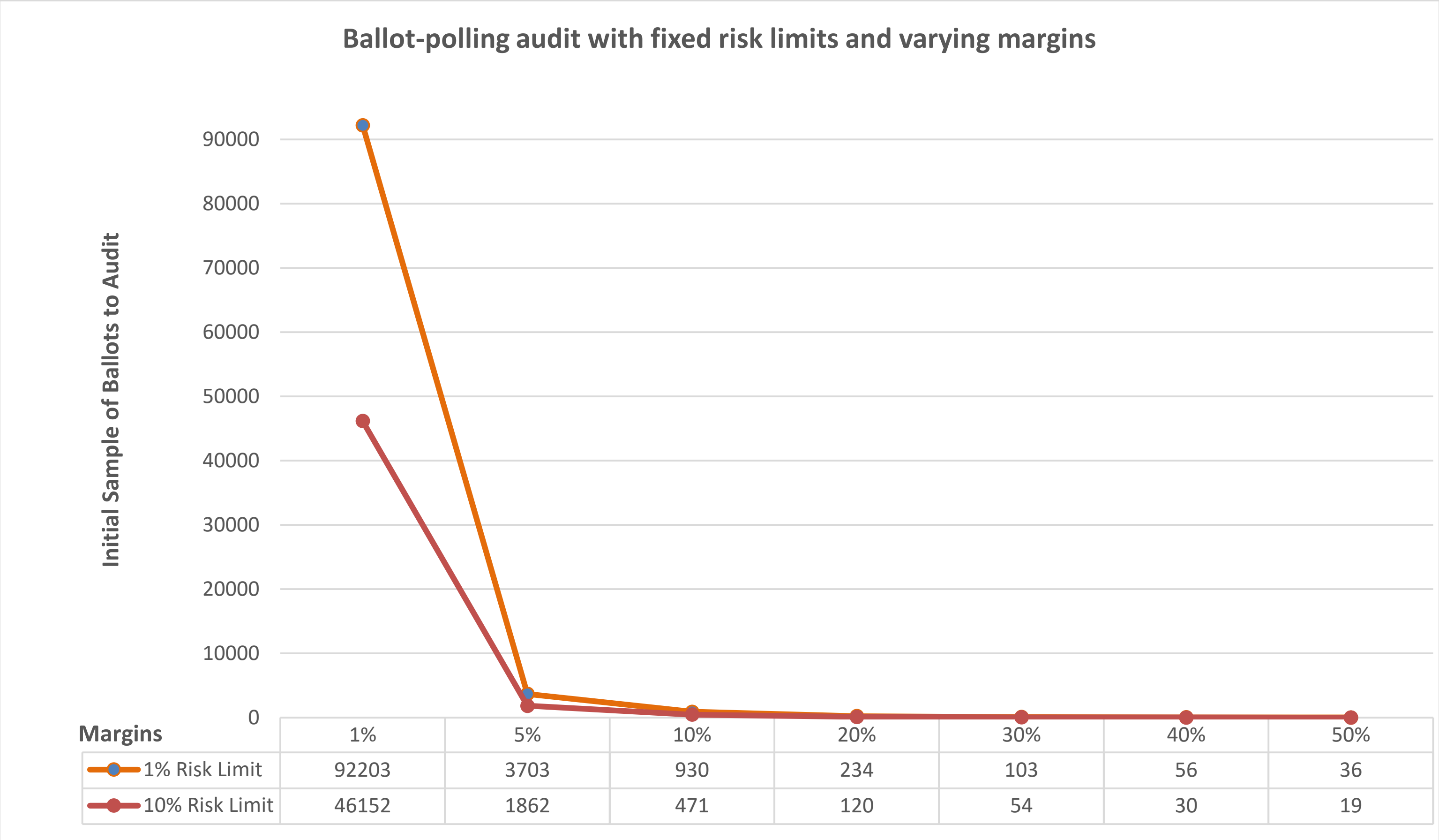
A Bayesian risk limit is a desired upper bound on the probability that the audit will make an error (by accepting an incorrect reported contest outcome as correct).

About Ballot-Polling RLAs

A ballot-polling RLA is similar to an exit poll. In this case, ballots (people) are randomly selected and tabulated (polled).

Pros	Cons
Minimal set-up costs	May require additional human resources
Does not require information from the voting system	Does not provide information about errors
Efficient for margins of 10% or greater	Inefficient for margins less than 10%

Ballot-Polling RLAs by the Numbers



Ballot-polling audit with fixed risk limits and varying margins

Margins	1%	5%	10%	20%	30%	40%	50%
1% Risk Limit	92203	3703	930	234	103	56	36
10% Risk Limit	46152	1862	471	120	54	30	19

About Bayesian Audits

Pros	Cons
Automatically provides a measure of risk at each point	It is simulation-based and software dependent
Does not require information from the voting system	Costs are unknown
Efficient for cross-jurisdictional contests and other voting methods	Requires a level of trust from the public since the computations are not transparent

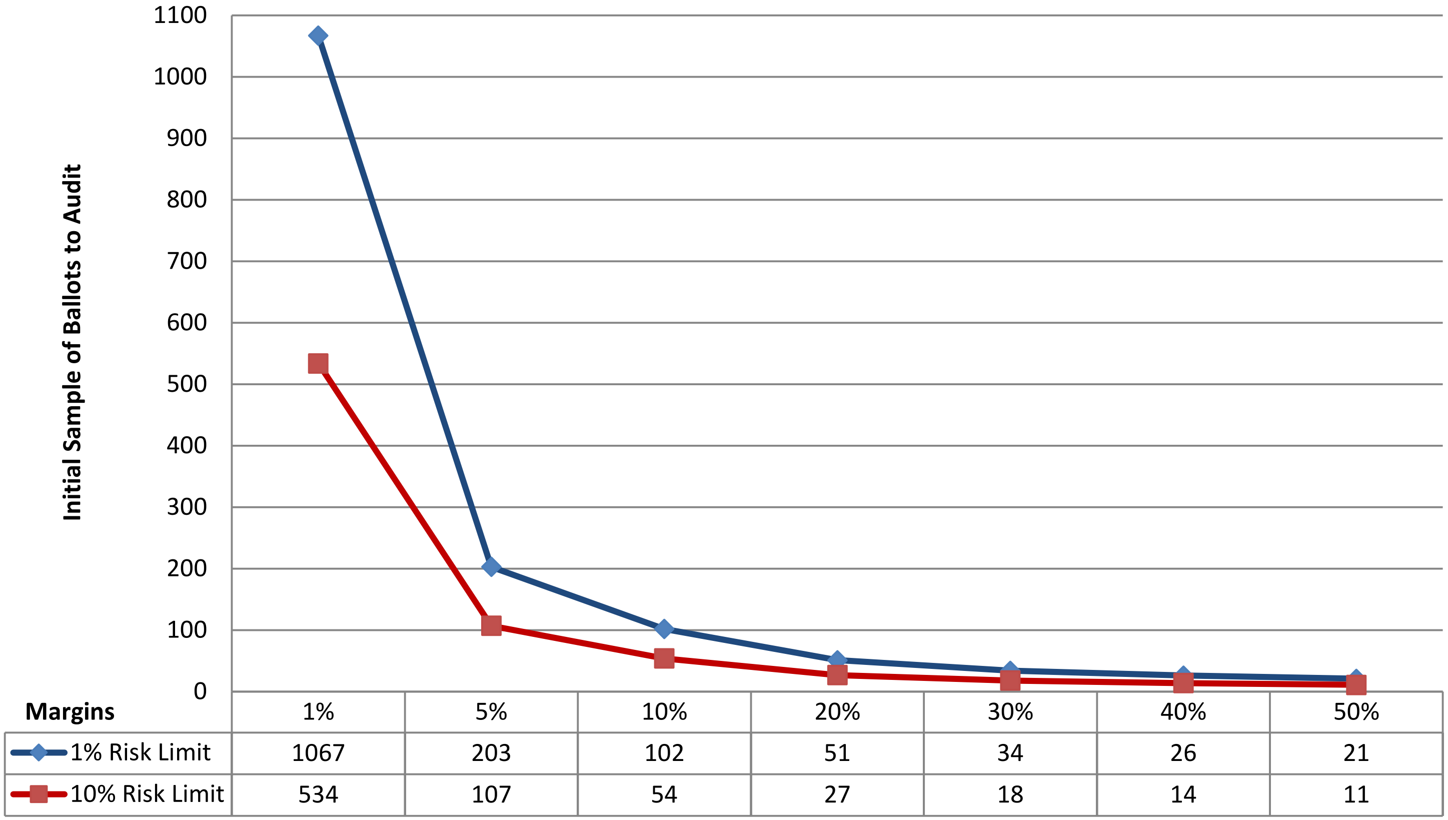
About Comparison RLAs

In a comparison RLA, individual ballots are randomly selected and compared to the CVR for each ballot.

Pros	Cons
Requires fewer human resources to conduct an audit	Depends on a voting system that can produce a CVR
Allows the auditor to correct any errors	Retrieving specific ballots can be difficult and time consuming
Efficient for margins of any size	Requires maintaining ballots in the exact order they are scanned, or imprinting numbers on the ballots

Comparison RLAs by the Numbers

Comparison audit with fixed risk limits and varying margins



Margins	1%	5%	10%	20%	30%	40%	50%
◆ 1% Risk Limit	1067	203	102	51	34	26	21
■ 10% Risk Limit	534	107	54	27	18	14	11

Uniform Audit Procedures

The uniform procedures that apply to the audit methods used are:

1. Maintain documented chain-of-custody for all ballots cast.
2. Create a ballot manifest, which is a document that describes how ballots are organized and stored.
3. Determine the risk limit.
4. Determine what contest(s) will be audited.
5. Decide what other utilities (software, calculator, spreadsheets, etc.) will be used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the auditor when the audit can stop.
6. Obtain a cast vote record (CVR) from the voting system (this is only used for comparison RLAs). A CVR is an export of data from the voting system showing how the voting system interpreted markings on every ballot.

Marion County Pilot Procedures

Ballot-Polling RLA

Using Dr. Stark's ballot-polling RLA tool[3] and the ballot manifest, we will obtain our initial sample of ballots to audit for each of the selected contests. The Marion County election staff will select the ballots, tabulate the results of each ballots, and the result will be entered into the audit tool. If the risk limit is not met with the initial sample of ballots, we will continue to select ballots until it is met.

Bayesian Audit

We will enter the sample of ballots obtained from the ballot-polling RLA into Dr. Rivest's Bayesian audit tool[4] which will compute the estimated probability of winning a full manual recount. Given a Bayesian risk limit of 5%, the Bayesian audit will stop when the auditor is at least 95% certain that the reported contest outcome is correct.

Marion County Pilot Procedures

Comparison RLA

We will use Dr. Stark's comparison RLA tool[5] and the ballot manifest to obtain our initial sample of ballots to audit. The Marion County election staff will compare the selected ballots to their CVRs. If there are no discrepancies, the audit will stop after the initial sample has been audited. If discrepancies are discovered, we may have to audit additional ballots (depending on the type of discrepancy).

Marion County Pilot Parameters

Risk Limit = 10%

Bayesian Limit = [***?***]

Contests to audit:

- 2016 Presidential
    - Estimated sample size (ballot-polling RLA) = ?
    - Estimated sample size (comparison RLA) = ?

- 2018 Republican U.S. Senate
    - Estimated sample size = [?]
    - Estimated sample size (comparison RLA) = ?

- 2018 Democrat Marion County Sheriff
    - Estimated sample size = [?]
    - Estimated sample size (comparison RLA) = ?

Sample Ballot Manifest

Precinct ID	Total # of Ballots	Precinct Batch ID	# of Precinct Ballots	Absentee Batch ID	# of Absentee Ballots
LA-03	400	LA-03P	300	LA-03A	100
WS-49	400	WS-49P	300	WS-49A	100
PE-39	600	PE-39P	400	PE-39A	200
WR-23	600	WR-23P	400	WR-23A	200
WS-69	600	WS-69P	400	WS-69A	200

What is Now

IC 3-11-13-38

Petition for confirmation of vote cast

Each county chairman for either of the major parties in the county may petition the county election board for confirmation of the vote cast on a ballot card voting system no earlier than the Saturday before an election and no later than the Thursday after an election. The petition may specify not more than five percent (5%)of the precincts or five (5) precincts, whichever is greater, in which a ballot card voting system was used for an audit under section 37 of this chapter.

What is Next

- Conduct additional pilots at counties of different sizes that use different voting systems.
- Determine what entity will serve as the central audit authority.
- Determine what method(s) will best serve Indiana.
- Draft laws and procedures for conducting an audit.
- Train local election officials on how to conduct audits.

- **Implement a statistics-based post-election audit.**

Notes

1. The ballot-polling and comparison RLAs were developed by Dr. Philip Stark, Associate Dean, Division of Mathematical and Physical Sciences at University of California - Berkeley, and Dr. Mark Lindeman, Adjunct Assistant Professor of Political Science at Columbia University. These methods have been tested by various jurisdictions around the U.S., and were implemented by Colorado beginning with the November 2017 election. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

2. Dr. Ron Rivest, Vannevar Bush Professor of Electrical Engineering and Computer Science at MIT, developed the Bayesian audit method that will be tested for the first time in Marion County, Indiana. https://arxiv.org/pdf/1801.00528.pdf

3. Ballot-Polling RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm#

4. Bayesian Audit Tool: http://audits.csail.mit.edu/

5. Comparison RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#

Contact

Jerome Lovato

jlovato@eac.gov

(202)805-4163

Social media

Email

listen@eac.gov

Facebook

Facebook.com/eacgov1

Twitter

@EACgov

Youtube Channel

Election Assistance Commission

Website

www.eac.gov

Voting System Technical Oversight Program at Ball State University (VSTOP)

Risk Limiting Audit (RLA) Pilot Report

August 2018

Risk Limiting Audit (RLA) Pilot
Marion County, Indiana
on
May 29-30, 2018

A Report to
the Indiana Secretary of State
August 15, 2018

By

Voting System Technical Oversight Program
(VSTOP)
Ball State University

Introduction and Background

Much has been reported in the news media in the last few years about the integrity of American elections and the security of voting equipment. This national discussion has centered on two key areas. First, the physical and cyber security of election equipment, and, second, the public's confidence in election equipment, the process of elections, and election outcomes. It is noteworthy that the Indiana Secretary of State Connie Lawson has been at the forefront of this discussion, both at the national and state levels, and has acted to address real and perceived threats to elections. There are several recent key events and items which are relevant to the present report. These include Indiana Governor's Executive Council on Cybersecurity, the Hoosier Survey, a recent report by the Center for American Progress, and the new Indiana election law addressing election security.

According to the website[1], "Signed by Governor Holcomb on Jan. 9, 2017, the Indiana Executive Council on Cybersecurity (Council) was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment. Led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, the Council is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders to collaboratively move "Indiana's cybersecurity to the Next Level." With 35 Council members and almost 250 advisory members, the Council will deliver a comprehensive strategy plan to Governor Holcomb by September 2018." One of the standing committees of the Council is for Elections which is chaired by Secretary Lawson.

In September of 2017, The Bowen Center for Public Affairs included survey questions on the 2017 Hoosier Survey regarding *perceived* voter confidence and problems with elections. The survey, which covered a wide variety of topics, was administered to a representative sample of 600 Indiana residents. The Hoosier Survey was conducted by Princeton Survey Research Associates International for Ball State University. The two questions germane to the present report and the responses appear in Tables 1 and 2 below.

Table 1
What level of confidence do you have that your vote in the last election was properly recorded and accurately counted?

Confidence Level	Percentage
Very confident	60%
Somewhat confident	23%
Not too confident	8%
Not confident at all	9%
Don't know/refused to answer	<1%

While 60% of the respondents felt "very confident" that their vote in the last election was properly recorded and accurately counted, nearly 40% of respondents were "somewhat," "not too" or "not at all" confident regarding their vote. This finding speaks to the power of perception regarding the integrity of elections. While elections are marked by general high levels of integrity, public perception is something which must be addressed along with physical and cyber protections for elections.

[1] https://www.in.gov/cybersecurity/2570.htm

Table 2 presents data on a related question and addressed perceived problems with elections. In response to this question, 53% of the respondents reported that the biggest problem with elections was "voter fraud" with 31% reporting it to be "denying eligible voters the right to vote."

Table 2

Thinking about elections in the United States, which of the following do you believe is a bigger problem?

Problem Area	Percentage
Voter fraud	53%
Denying eligible voters the right to vote	31%
Both equally	7%
Neither	4%
Don't know/refused to answer	4%

Perceptions, whether or not grounded in reality, are important to consider when addressing elections and election integrity. Thus, one part of the equation in addressing election integrity is the physical and cyber security needed to protect elections while the other is addressing the public perceptions which exist around elections. In addition to issues raised through public perceptions, there are also special interest organizations which have examined elections and election security. One of these is the Center for American Progress (CAP).

On February 15, 2018 the Voting System Technical Oversight Program (VSTOP) received a communication from General Counsel Jerry Bonnet in the Office of the Indiana Secretary of State. Mr. Bonnet sent VSTOP a copy of the Center for American Progress (CAP) Report *Election Security in All 50 States* - *Defending America's Elections.* Mr. Bonnet asked VSTOP to review the CAP report and comment on the report and the methodology that led to Indiana receiving a "grade of F." VSTOP's response presented an assessment of the CAP report and the methodology employed by the authors to grade the 50 states on how the states were "faring in meeting even the minimum standards necessary to help secure their elections." The report awarded points based on the assessment of states' activities in seven categories: Cybersecurity standards for voter registration systems; Voter-verified paper audit trail; Post-election audits; Ballot accounting and reconciliation; Return of voted paper absentee ballots; Voting machine certification requirements; and Pre-election logic and accuracy testing. VSTOP's review found that the categories and the weights given to the categories seemed arbitrary, with no clear justification provided. Emerging activities such as post-election audits, which few states had implemented at the time of the report, were given three times the weight than other important and established election security areas such as voting machine certification requirements. States that used DREs in even a *single* jurisdiction were given an unsatisfactory rating in one of the categories, which seemed a harsh criticism of a practice currently followed by several states. Of greater concern, VSTOP's review indicated that the authors seemed unaware of Indiana's achievements in the seven categories. In some cases, the authors used outdated data, while in others even impressive data mentioned in the report was not reflected in the points or ratings awarded to Indiana. VSTOP concluded that the grade of "F" awarded to Indiana did not reflect a true and accurate picture of the many achievements in Elections Security and in the seven categories explored by the CAP authors. One of the areas in the CAP report given heavy emphasis was the use of Risk-Limiting Audits (RLAs) as a means of post-election audits of election outcomes. VSTOP and the Indiana Secretary of State were actively exploring the use of RLAs in the state when the report was being constructed and were also planning the first RLA pilot in the state.

On May 29 and 30, 2018, the VSTOP Team conducted Indiana's first RLA pilot in Marion County, Indiana. This pilot was carried out in collaboration with Mr. Jerome Lovato, Certification Program Specialist at the US Election Assistance Commission (EAC), Dr. Ronald L. Rivest, Institute Professor at MIT and a member of the Caltech/MIT Voting Technology Project, and Ms. Mayuri Sridhar, a Research and Innovation Scholar at MIT. Appendix A provides the handout for the RLA packet that was distributed to all parties. VSTOP could not have completed this work without the generous help and cooperation of Marion County Clerk Myla Eldridge and her elections staff, Ms. Brienne Delaney, Director of Elections & Ms. Jenny Troutman, Deputy Director of Elections. Indiana Secretary of State Connie Lawson, Chief of Staff and Deputy Secretary Brandon Clifton, their staff, Indiana Election Division Co-Directors Brad King and Angie Nussmeyer were all involved in the organization of this RLA Pilot. We appreciate the visit by the Secretary, Brandon Clifton, Brad King, Angie Nussmeyer, and Valerie Warycha (Deputy Chief of Staff and Director of Communications & Media Contact) at the audit site.

Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Elections in Colorado are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California Secretary of State recently completed a three-year pilot program that audited contests of varying size in counties throughout the state. In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

While there is a large set of references on RLAs, the following two provide comprehensive introductions and details.

- A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
- A Bayesian Method for Auditing Elections https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally, there are two types of statistical methods: RLA and Bayesian. These are described below.

In the ballot polling sampling, one randomly draws ballots, examines ballots by hand and tallies results for each ballot. For ballot comparison, ballots are randomly drawn, examined by hand and each ballot is compared to its cast vote record (CVR). For batch polling, one randomly draws batches, examines results by hand, and tallies results for each batch. Finally, for batch comparison, one randomly draws batches, examines ballots by hand, tallies results for each batch and compares each batch to its batch report produced by the voting system. Ballot-level audits are more efficient than batch-level since they require examining fewer ballots. A comparison audit is more efficient but requires CVRs. Polling can be used if CVRs are not available.

The Stark RLA provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome. The risk limit is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome. The Stark audit tool can be found at the following link:
https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

A **Bayesian audit** is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else determines the correct contest outcome. A **Bayesian risk limit** is a desired upper bound on the probability that the audit will make an error (by accepting an incorrectly reported contest outcome as correct). The Bayesian audit tool can be found at the following link:
https://arxiv.org/pdf/1801.00528.pdf

The Stark RLA is more popular and statistically rigorous. The Bayesian is more flexible and can be used in non-standard situations.

RLAs are valuable because these can detect problems with election outcomes, with a high degree of statistical confidence, without having to engage in an expensive and time-consuming full recount unless it is absolutely necessary. Further, the outcomes from RLAs can enhance voter confidence that votes were correctly counted and tabulated. Moreover, RLAs serve as a check on the integrity of election outcomes based on statistical methods which confirm winners.

The Marion County, Indiana RLA Pilot

On the afternoon of May 29, 2018, VSTOP and the RLA team prepared for the RLA by obtaining ballots collected from selected precincts which would be used to draw samples of ballots for the "Ballot Polling RLA" as well as a cast vote record for a "Comparison RLA."

The RLA Team audited three races in the RLA pilot. These were:

- 2016 Presidential Election (5 precincts) – 2602 ballots cast (see Appendix B - Section 1 for full RLA details)
    - Needed to audit 61 ballots. Used Ballot Polling method to select this sample
    - Stark and Bayesian methods worked as expected and confirmed the "Clinton" outcome in the Marion County precincts with high levels of statistical assurance

- 2018 Primary Democratic Sheriff (10 Precincts) – 1747 ballots cast (see Appendix B - Section 2 for full RLA details)
    - Needed to audit 169 ballots. Used a combination of Three-Cut and Ballot Polling methods to select this sample
    - Stark and Bayesian methods worked as expected and likely would have confirmed the "Forestal" outcome with high levels of statistical assurance
    - However, these audits were ceased early due to time constraints

- 2018 Republican U.S. Senator (Comparison Polling Audit) – 1490 ballots cast (see Appendix B - Section 3 for full RLA details)
    - Due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method
    - Simulated CVRs were used for comparison
    - The audit ceased early but did not contradict the election outcome for "Braun" as the winner

The first RLA confirmed Clinton as the winner in the precincts audited for the 2016 general election for president. This was a fully completed RLA. The next two RLAs, although ceased early due to time constraints, did not contradict what would be expected in the selected precincts with Forestall the winner for the Democratic Sheriff's primary and Braun as the winner in the Republican U.S. Senate primary. As one examines the small number of ballots which needed to be sampled and examined for each of the three RLAs, one can appreciate the power of these methods as accurate predictors of election outcomes.

The experience was positive and valuable in learning how RLAs operate in the field. It is noteworthy that this was the first time that the Bayesian Audit Method was used in the field.

Jessica Martin, VSTOP Project Manager observed an RLA held in Denver County, Colorado July 5-6, 2018. Her reflections on this experience appear in Appendix C.

Conclusion

VSTOP is comfortable moving forward with additional pilot audits in the state at the Secretary's discretion. VSTOP believes at least one additional pilot is necessary since two of the races audited were ceased early due to time constraints. Nevertheless, there is no reason to believe the outcome would have been contradicted based on the actual winners given how well the audits were progressing given real-time results. VSTOP believes it would be a good practice to spend two full days to completely finish a future pilot audit in a different county with paper ballots in order to test the methods again and to gain additional experience with Risk-Limiting Audits. Additionally, there is value in completing RLAs on a variety of voting systems and vendors. With more experience in conducting RLAs, VSTOP will explore making recommendations to the Secretary regarding the feasibility and benefits of implementing RLAs statewide where applicable.

Acknowledgment

The VSTOP Team wishes to acknowledge and thank Secretary Lawson and her staff, Indiana Election Division, Jerome Lovato, Professor Ron Rivest, Mayuri Sridhar and the Marion County Clerk's Office staff (especially Brienne Delaney and Jenny Troutman) for their support and assistance with this project and report.

Appendix A

Post-Election Risk Limiting Audit Pilot

Marion County Indiana
May 30, 2018

An Introduction

A Collaboration between Marion County Office of the Clerk, Office of the Indiana Secretary of State, Indiana Governor's Executive Council on Cybersecurity, U.S. Election Assistance Commission, Caltech/MIT Voting Technology Project, and the Voting System Technical Oversight Program (VSTOP) at Ball State University

Introduction

In January 2017, U.S. Elections Systems were designated as part of the nation's critical infrastructure by the United States Department of Homeland Security. Also, in January 2017, Indiana Governor Holcomb signed an Executive Order to continue the Indiana Executive Council on Cybersecurity (IECC) (https://www.in.gov/cybersecurity/2570.htm). The Executive Council comprises ten committees and several working groups. The Elections Committee of the Council is chaired by the Indiana Secretary of State Hon. Connie Lawson. Dr. Jay Bagga, Co-Director of the Voting System Technical Oversight Program (VSTOP) serves as an Advisory Member to this Council and is a member of the Elections Committee.

One of the deliverables for the Elections Committee is to create a **Post-election risk limiting audit (RLA)** protocol proposal. As a component of this activity, VSTOP proposed conducting a pilot RLA in some Indiana counties. VSTOP began discussing the RLA process with Jerome Lovato, Election Technology Specialist at the U. S. Election Assistance Commission.

VSTOP considered several counties for such an audit. It is important to note that only jurisdictions with Voter Verifiable Paper Ballots are amenable to RLAs. VSTOP selected Marion County for this and a variety of other reasons, including its high voter registration. With the approval of Secretary Lawson and the Co-Directors of the Indiana Election Division, VSTOP held discussions with Marion County Elections Officials to discuss a potential partnership. VSTOP was pleased that in April 2018 Marion County agreed to be our partner for this endeavor.

The RLA Pilot will be conducted in Marion County, Indianapolis on May 30, 2018. In planning for this audit, Mr. Lovato proposed that the RLA Pilot include methods proposed by Dr. Philip B. Stark (Berkeley) and Dr. Ronald L. Rivest (MIT). These methods, the RLA method and the Bayesian Method will be used in the pilot for several races from the 2016 and 2018 elections. The races we are planning to audit are the Presidential Race from the November 2016 General Election, the U.S. Senate Race from the November 2018 Republican Primary Election, and the Sheriff Race from the 2018 Democratic Primary Election.

Marion County uses the ES&S EVS 5.2.2.0 which is an OpScan Voting System. This voting system is used in five other Indiana counties. The experience gained from a successful pilot audit can serve as the basis for RLA replication in other counties.

The RLA Pilot Team has relied on many of the lessons learned from the State of Colorado which was the first state to mandate Risk Limiting Audits as part of their post-election audit procedures. At this time not all Counties in Indiana have the capability to conduct a Post-Election Audit because we are not aware of any Direct Recording Electronic (DRE) Voting machines certified in the state of Indiana that produce a voter-verifiable paper audit trail.

The VSTOP Team, Mr. Lovato, Dr. Rivest, as well as members of Marion County Elections Officials have held weekly WebEx planning meetings since the beginning of May. The RLA Pilot Team will meet at the Marion County Election Service Center on the afternoon of May 29th to organize and prepare for the Audits to be held on May 30th.

Based on a process assessment and the outcome of this initial Post-Election Audit initiative, VSTOP will advise the Indiana Secretary of State and the Governor's Indiana Executive Council on Cybersecurity regarding the future potential uses of post-election audits within the state of Indiana.

A Brief Overview of Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology. There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally, there are two types of statistical methods: RLA and Bayesian.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Coordinated elections are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California secretary of state recently completed a three-year pilot program that audited contests of varying size in counties throughout the state.

In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

References

A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012.
https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

A Bayesian Method for Auditing Elections
https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

For more details please see the PowerPoint presentation by Jerome Lovato at the end of this document.

Marion County Post-Election Audit Pilot Agenda

Location: Election Service Center at 3737 E. Washington St., Indianapolis, IN 46201

Day 1 – May 29th 12:00 PM – 4:30PM

12:00 PM VSTOP: Introductions
12:15 PM County: Review state/county guidelines for handling ballots and accessing restricted areas
12:30 PM County: Walk through procedure for organizing and storing ballots
1:00 PM J. Lovato: Provide Risk Limiting Audit (RLA) overview to county officials (Q&A)
1:30 PM Create/Review Ballot Manifests, organize ballots for audits
3:00 PM Ensure Primary ballots are separated by Democratic and Republican categories, nonpartisan, if applicable
4:00 PM Phone Conference with Secretary Lawson

Day 2 – May 30th 8:30 AM – 3:30 PM

8:30 AM VSTOP: Introductions
J. Lovato: Risk Limiting Audit overview
Dr. Rivest: Bayesian Audit Method
9:15 AM Ballot Polling Audit of 2016 Presidential Race in Precincts LA-03, WS-49, PE-39, WR-23 and WS-69
10:00 AM Break
10:15 AM Ballot Polling Audit of 2018 Republican U.S. Senate Race in Precincts PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27
11:00 AM Ballot Polling Audit of 2018 Democrat Marion County Sheriff in Precincts PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27
Noon Remarks by Secretary Connie Lawson
12:15 PM Lunch Break
1:30 PM Bayesian Audit of 2016 Presidential, 2018 Primary R-U.S. Senate Race 2018 Primary D-Sheriff Race
2:15 PM J. Lovato: Example/demo of comparison audit procedures
3:00 PM Conclusion

The RLA Pilot Team

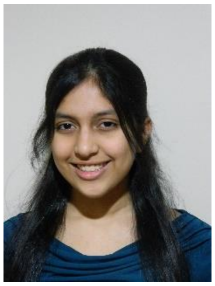
Jerome Lovato, Election Technology Specialist, U. S. Election Assistance Commission (EAC)

Jerome received his Bachelor of Science in Electrical Engineering from the University of Colorado at Denver. After working as an electrical engineer in the consumer electronics industry for six years, he worked as a Voting Systems Specialist at the Colorado Secretary of State's office for 10 years as a Voting System Certification Lead and Risk-Limiting Audit Project manager. Currently, he is an Election Technology Specialist for the U.S. Election Assistance Commission. Jerome led the team in Colorado that employed the RLA method. The following link is a gentle introduction to this method: https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Dr. Ronald L. Rivest, Institute Professor at MIT

Professor Rivest is an Institute Professor at MIT. He joined MIT in 1974 as a faculty member in the Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. He is a co-author (with Cormen, Leiserson, and Stein) of the text, *Introduction to Algorithms*. He is also a founder of RSA Data Security, now named RSA Security (the security division of EMC), Versign, and Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, electronic voting, and algorithms. A paper on the Bayesian method can be found at: https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

Mayuri Sridhar, Research and Innovation Scholar, MIT



Mayuri Sridhar is a Master's student studying Artificial Intelligence at MIT. She completed her undergraduate degree at MIT, double majoring in computer science and mathematics. Her research, under Professor Rivest's supervision, focuses on statistics and optimization, applied to election audits.

Marion County Clerk's Office

Myla A. Eldridge, County Clerk
Brienne Delaney, Director of Elections
Jenny Troutman, Deputy Director of Elections
Joanna Alexander, Absentee Administrator
Colin Claycomb, Ballot Administrator
Rhonda Hawkins, Service Center Manager
and other county staff personnel

The VSTOP Team

Dr. Jay Bagga and Dr. Bryan Byers, VSTOP Co-Directors
Jessica Martin, VSTOP Project Manager
Mani Kilaru, VSTOP IT Specialist
Molly Owens, VSTOP Graduate Assistant
Contact: VSTOP@bsu.edu

Statistical Post-Election Audit Pilot

at Marion County, IN

Jerome Lovato, Election Technology Specialist

U.S. Election Assistance Commission

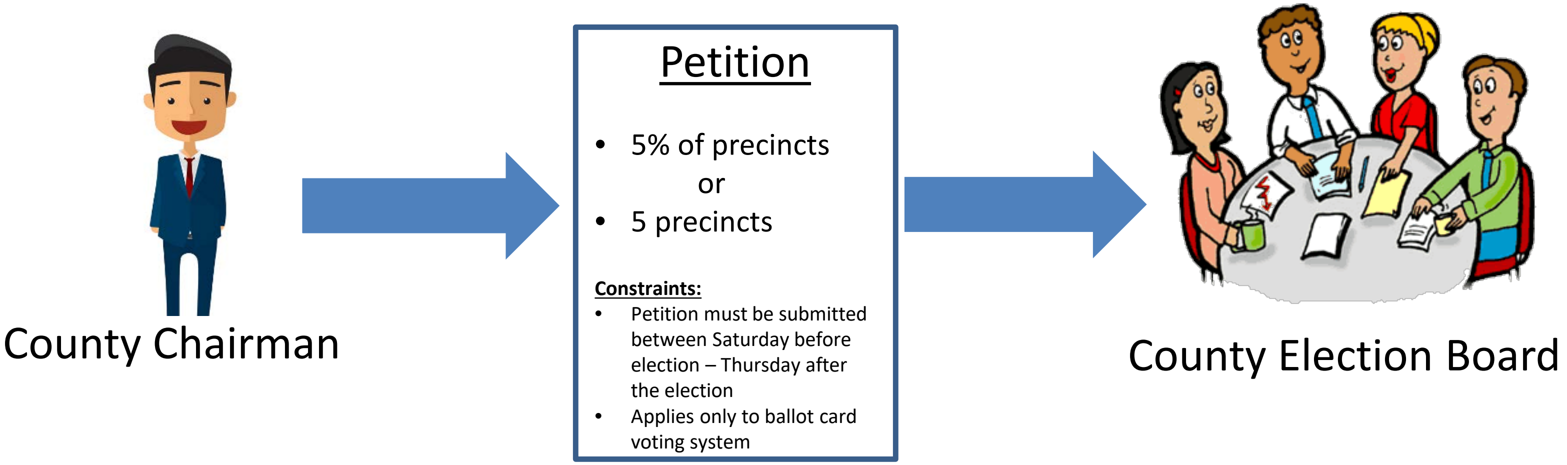
Let’s talk about statistics-based post-election audits.

What problem are we trying to solve?
What is RLA?
How long will it take?
How much work is involved?
How much will it cost?
Who will administer the audit?

Indiana Post-Election Audit

IC 3-11-13-38

Petition for confirmation of vote cast



County Chairman

Petition

- 5% of precincts

or

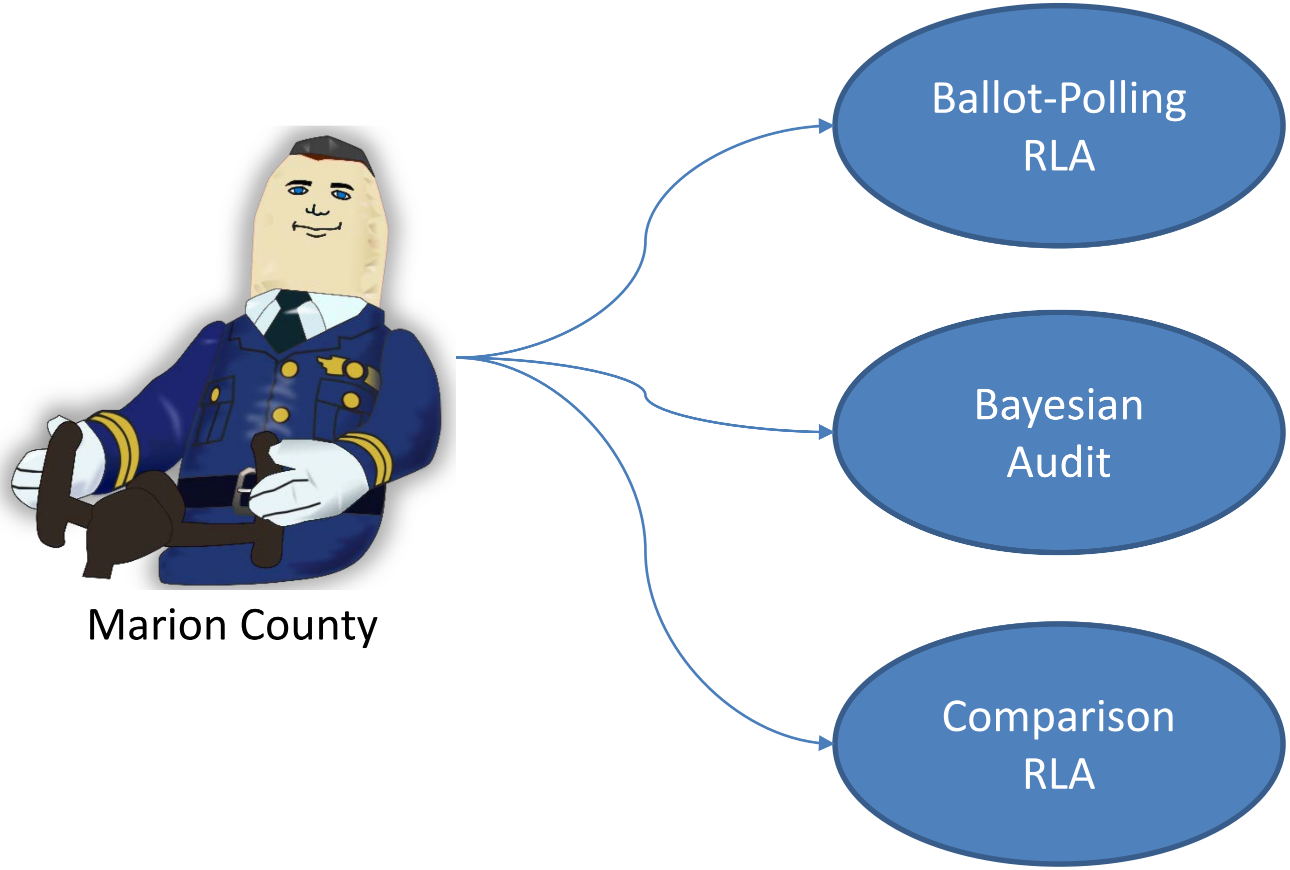
- 5 precincts

Constraints:

- Petition must be submitted between Saturday before election – Thursday after the election
- Applies only to ballot card voting system

County Election Board

Marion County Pilot



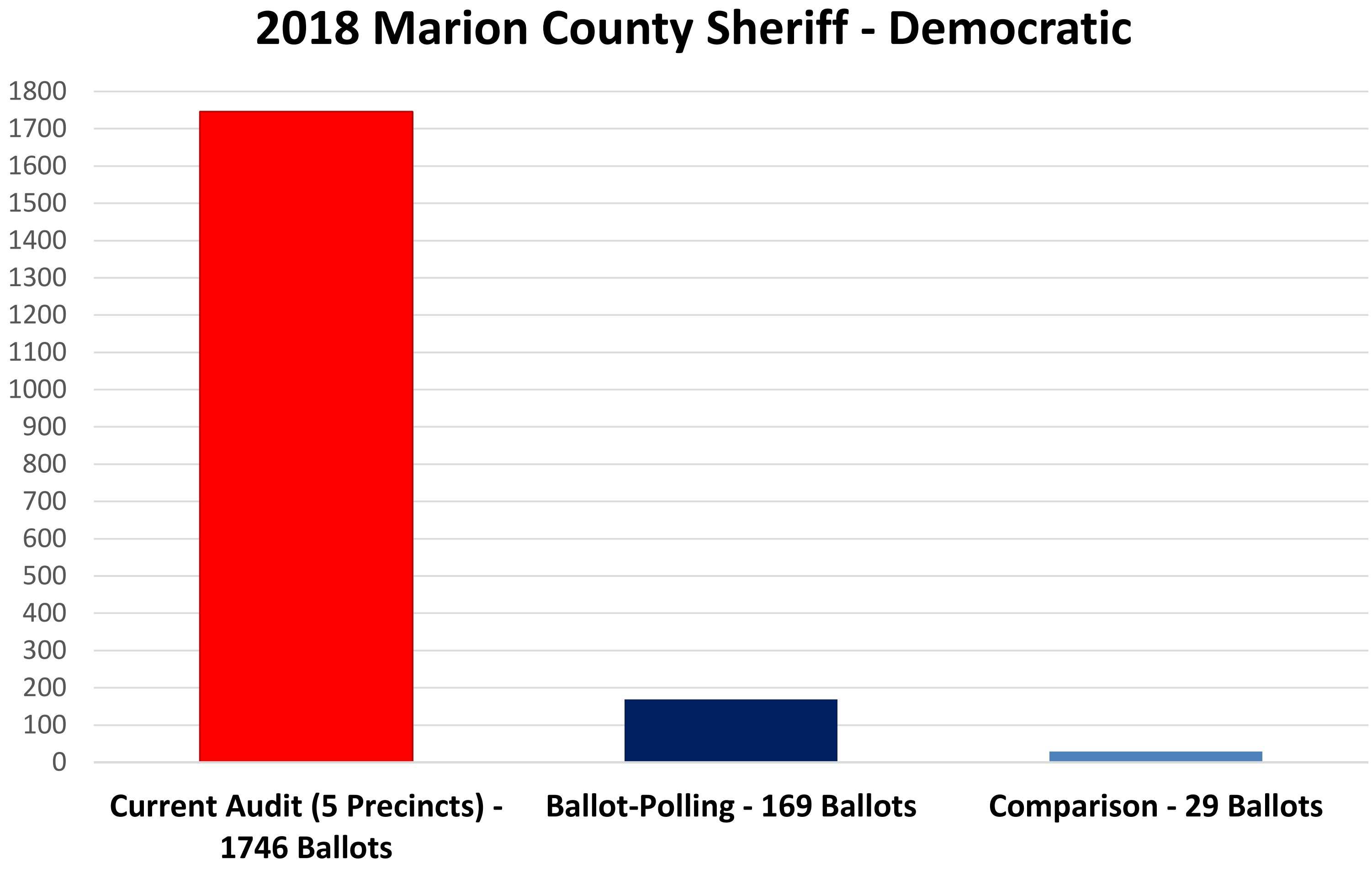
Marion County

Ballot-Polling RLA

Bayesian Audit

Comparison RLA

RLA Workload Example



Statistical Audit Methods - Terminology

A **risk-limiting audit (RLA)** provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.[1] There are two main types of RLAs: ballot-polling and comparison.

The **risk limit** is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome.

A **Bayesian audit** is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else finds out the correct contest outcome.[2]

A **Bayesian risk limit** is a desired upper bound on the probability that the audit will make an error (by accepting an incorrect reported contest outcome as correct).

Sampling Methodologies

Ballot Polling

- Randomly draw ballots
- Examine ballots by hand
- Tally results for each ballot

Ballot Comparison

- Randomly draw ballots
- Examine ballots by hand
- Compare each ballot to its cast vote record (CVR)

Batch Polling

- Randomly draw batches
- Examine ballots by hand
- Tally results for each batch

Batch Comparison

- Randomly draw batches
- Examine ballots by hand
- Tally results for each batch
- Compare each batch to its batch report produced by the voting system

Statistical Methodologies

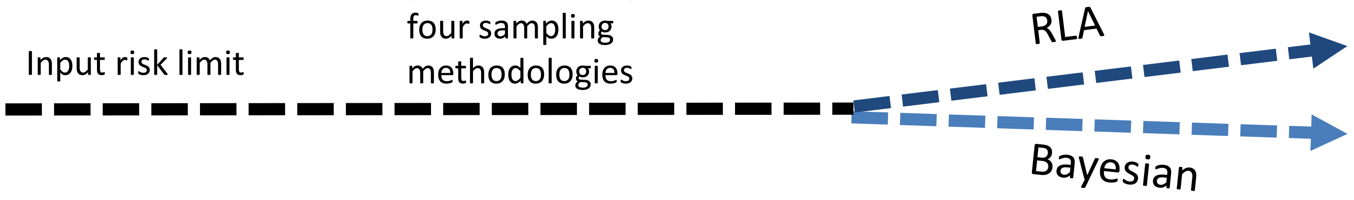
There are two statistical methodologies that describe how the statistical data obtained from the sampling methodologies will be used.

Risk-Limiting Audit

Bayesian Audit

Statistical Methodologies Cont.

The statistical methodology determines whether the audit can stop, or whether more data needs to be obtained. The statistical assurances provided are slightly different between these two types.

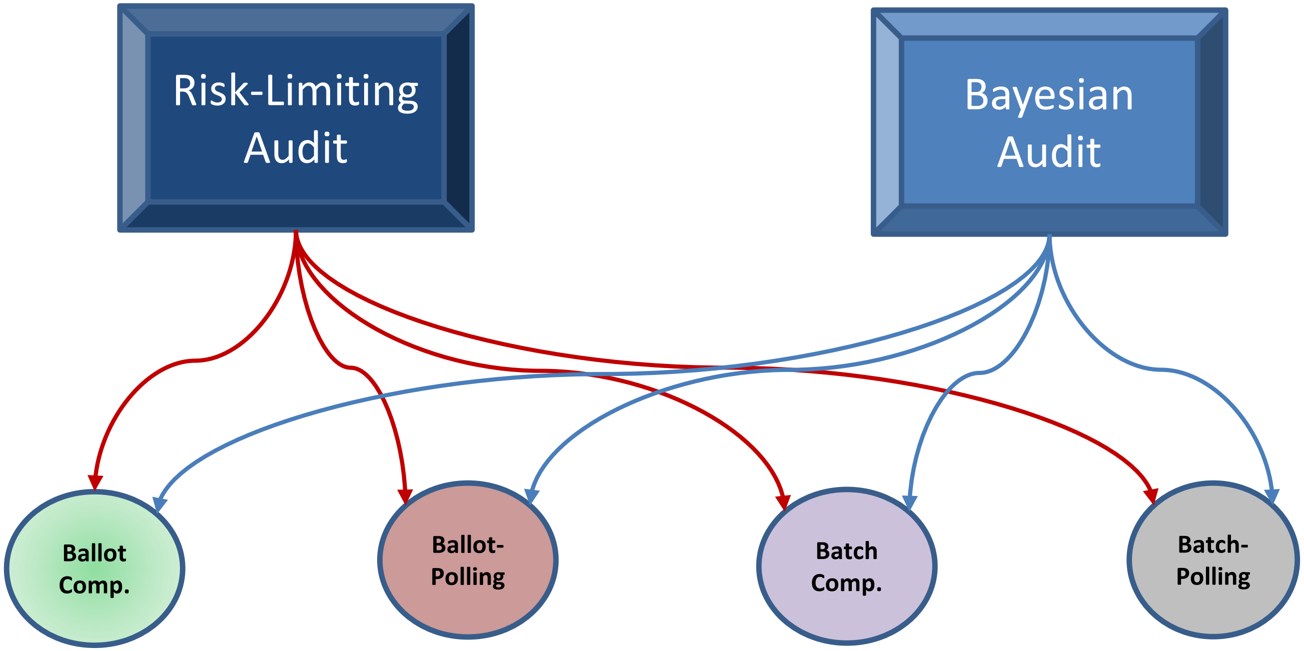


Input risk limit

Each statistical methodology can be paired with any of the four sampling methodologies

Statistical Methodologies Cont.

There are at least eight different kinds of audits one may run, depending on the choice of sampling methodology and statistical methodology.



Statistical Methodologies Cont.

Comparison vs Polling

- Comparison is more efficient, but requires CVRs
- Polling can be used if CVRs are not available

Ballot-Level vs Batch-Level

- Ballot-level audits are more efficient than batch-level since they require examining less ballots.

RLA vs Bayesian

- RLA is more popular and statistically rigorous
- Bayesian is more flexible and can be used in non-standard situations

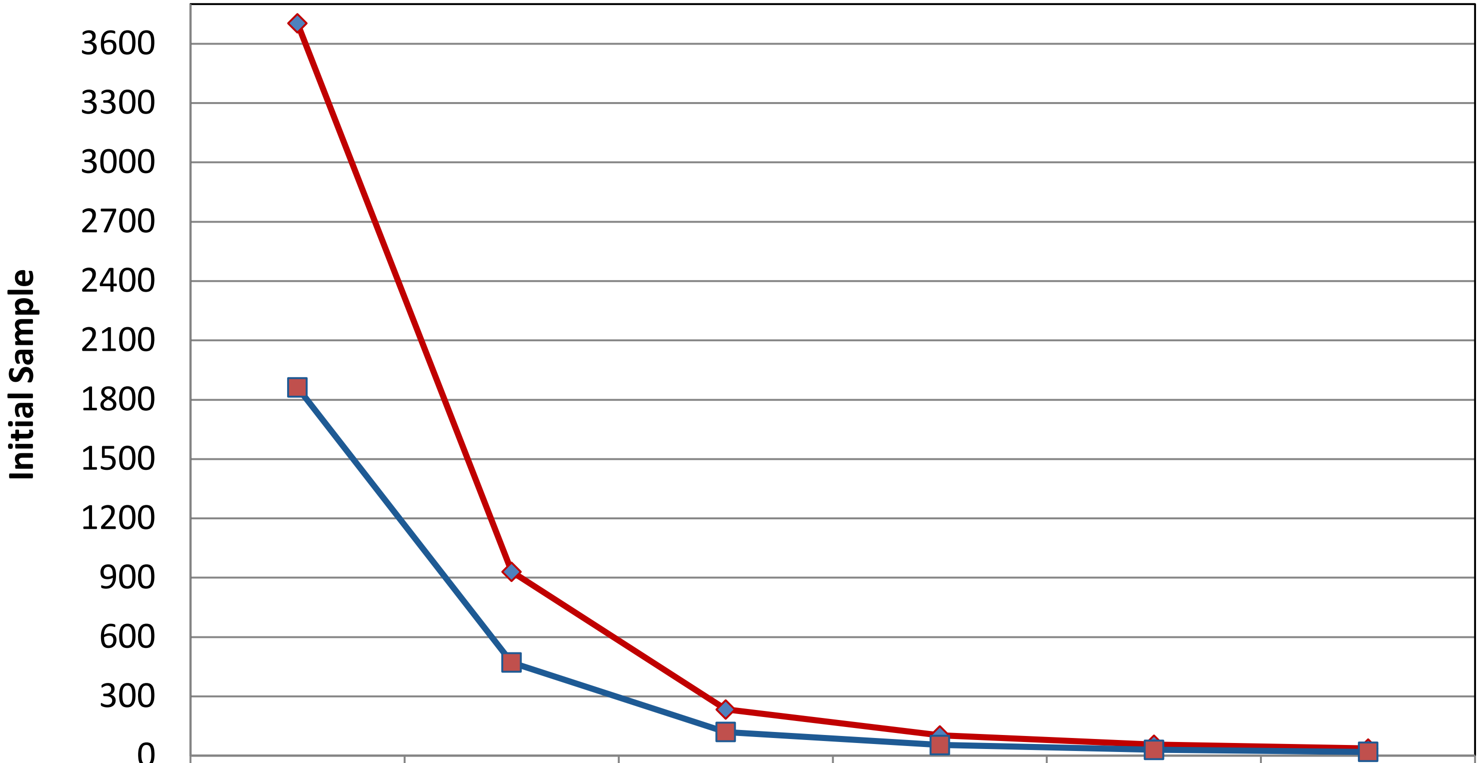
About Ballot-Polling RLAs

A ballot-polling RLA is similar to an exit poll. In this case, ballots (people) are randomly selected and tabulated (polled).

Pros	Cons
Minimal set-up costs	May require additional human resources
Does not require information from the voting system	Does not provide information about errors
Efficient for margins of 10% or greater	Inefficient for margins less than 10%

Ballot-Polling RLAs by the Numbers

Ballot-polling RLA with fixed risk limits and varying margins



Margin	5%	10%	20%	30%	40%	50%
◆ 1% Risk Limit	3703	930	234	103	56	36
■ 10% Risk Limit	1862	471	120	54	30	19

About Bayesian Audits

Pros	Cons
Automatically provides a measure of risk at each point	It is simulation-based and software dependent
Does not require information from the voting system	Costs are unknown
Efficient for cross-jurisdictional contests and other voting methods	Requires a level of trust from the public since the computations are not transparent

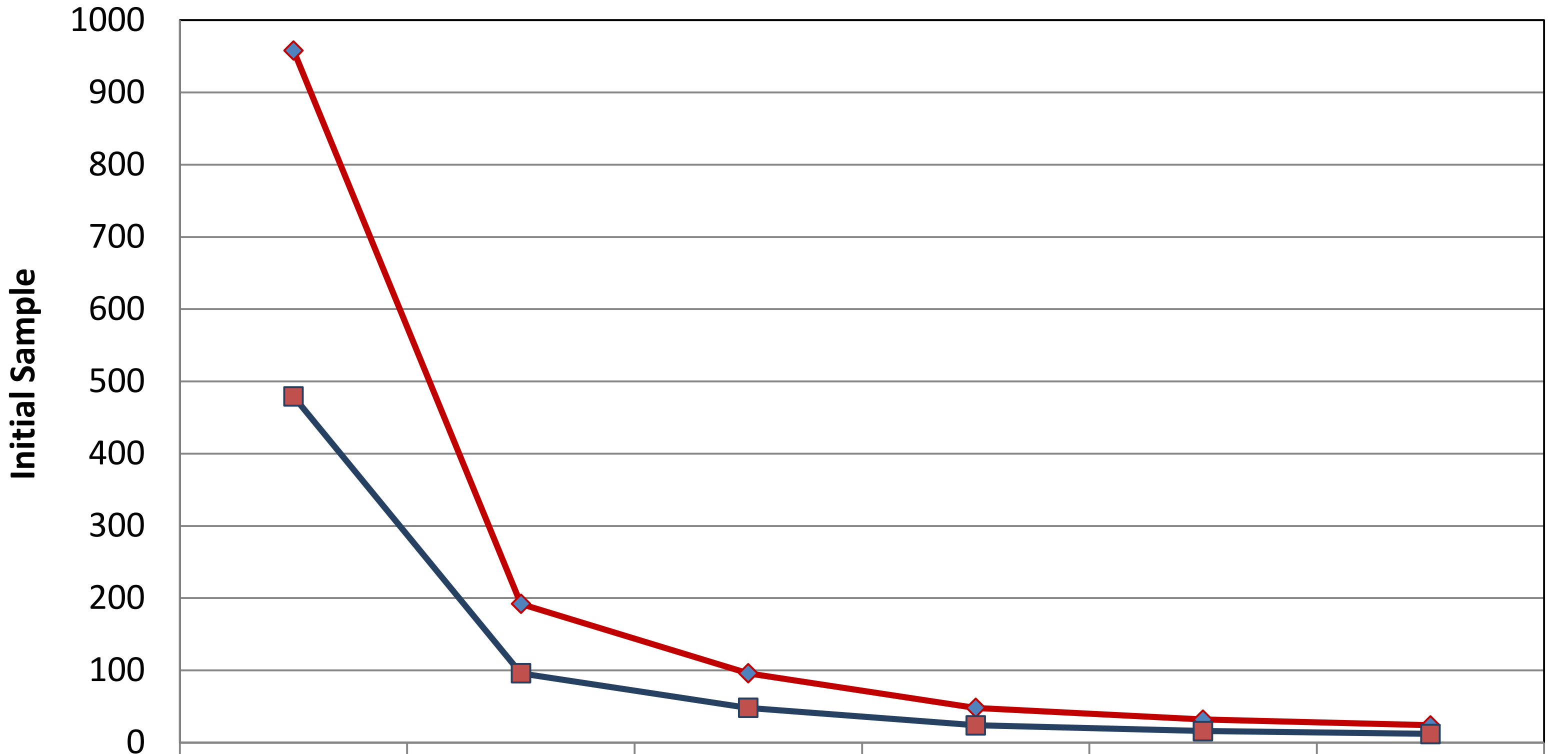
About Comparison RLAs

In a comparison RLA, individual ballots are randomly selected and compared to the CVR for each ballot.

Pros	Cons
Requires fewer human resources to conduct an audit	Depends on a voting system that can produce a CVR
Allows the auditor to correct any errors	Retrieving specific ballots can be difficult and time consuming
Efficient for margins of any size	Requires maintaining ballots in the exact order they are scanned, or imprinting numbers on the ballots

Comparison RLAs by the Numbers

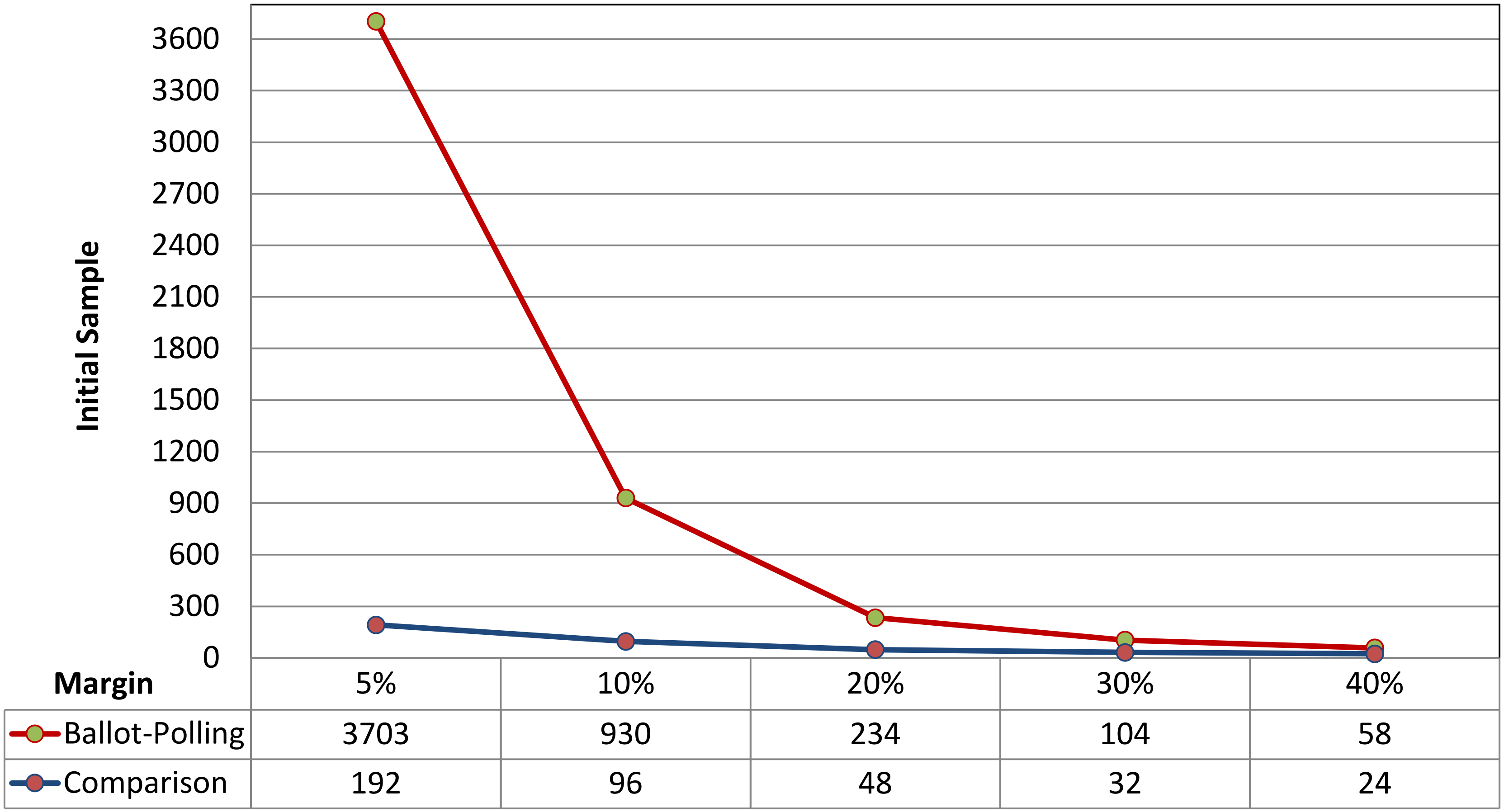
Comparison RLA with fixed risk limits and varying margins



Margin	1%	5%	10%	20%	30%	40%
1% Risk Limit	958	192	96	48	32	24
10% Risk Limit	479	96	48	24	16	12

Ballot-Polling vs Comparison RLAs

Ballot-Polling vs Comparison RLA with 1% risk limit and varying margins



Margin	5%	10%	20%	30%	40%
Ballot-Polling	3703	930	234	104	58
Comparison	192	96	48	32	24

Uniform Audit Procedures

The uniform procedures that apply to the audit methods used are:

1. Maintain documented chain-of-custody for all ballots cast.
2. Create a ballot manifest, which is a document that describes how ballots are organized and stored.
3. Determine the risk limit.
4. Determine what contest(s) will be audited.
5. Decide what other utilities (software, calculator, spreadsheets, etc.) will be used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the auditor when the audit can stop.
6. Obtain a CVR from the voting system (this is only used for comparison RLAs). A CVR is an export of data from the voting system showing how the voting system interpreted markings on every ballot.

Marion County Pilot Procedures

Ballot-Polling RLA

Use Dr. Stark's ballot-polling RLA tool[3] and the ballot manifest.

1. Enter the contest information
2. Enter a random seed for the pseudo random number generator
3. Obtain the initial sample of ballots to audit
4. Marion County election staff will:
    1. Select the ballots
    2. Hand tally the results for each ballot
5. Enter the hand tally results into the audit tool
6. If the risk limit is met then the audit will stop.
7. If the risk limit is not met then additional ballots will be selected.

Marion County Pilot Procedures Cont.

Bayesian Audit

Use Dr. Rivest's Bayesian audit tool[4] and the initial sample from the ballot-polling RLA.

1. Enter the sample of ballots obtained from the ballot-polling RLA into the Bayesian audit tool
   1. The Bayesian audit tool will compute the estimated probability of winning a full manual recount. Given a Bayesian risk limit of 5%, the Bayesian audit will stop when the auditor is at least 95% certain that the reported contest outcome is correct.

Marion County Pilot Procedures Cont.

Comparison RLA

Use Dr. Stark's comparison RLA tool[5] and the ballot manifest

1. Enter the contest information
2. Enter a random seed for the pseudo random number generator
3. Obtain the initial sample of ballots to audit
4. Marion County election staff will:
    1. Select the ballots
    2. Compared the selected ballots to their CVRs
5. If the risk limit is met then the audit will stop.
6. If the risk limit is not met then additional ballots will be selected.

Marion County Pilot Parameters

Risk Limit = 10%

Bayesian Limit = 5%

Contests to audit:

- 2016 Presidential
  - Estimated sample size (ballot-polling RLA) = 62
  - Estimated sample size (comparison RLA) = 18

- 2018 Republican U.S. Senate
  - Estimated sample size (ballot-polling RLA) = 242
  - Estimated sample size (comparison RLA) = 35

- 2018 Democrat Marion County Sheriff
  - Estimated sample size (ballot-polling RLA) = 169
  - Estimated sample size (comparison RLA) = 29

Sample Ballot Manifest

Precinct ID	Total # of Ballots	Precinct Batch ID	# of Precinct Ballots	Absentee Batch ID	# of Absentee Ballots
LA-03	400	LA-03P	300	LA-03A	100
WS-49	400	WS-49P	300	WS-49A	100
PE-39	600	PE-39P	400	PE-39A	200
WR-23	600	WR-23P	400	WR-23A	200
WS-69	600	WS-69P	400	WS-69A	200

What is Next?

- Conduct additional pilots at counties of different sizes that use different voting systems.
- Determine what entity will serve as the central audit authority.
- Determine what method(s) will best serve Indiana.
- Draft laws and procedures for conducting an audit.
- Train local election officials on how to conduct audits.

- **Implement a statistics-based post-election audit.**

Notes

1. The ballot-polling and comparison RLAs were developed by Dr. Philip Stark, Associate Dean, Division of Mathematical and Physical Sciences at University of California - Berkeley, and Dr. Mark Lindeman, Adjunct Assistant Professor of Political Science at Columbia University. These methods have been tested by various jurisdictions around the U.S., and were implemented by Colorado beginning with the November 2017 election. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

2. Dr. Ron Rivest, Institute Professor at MIT, developed the Bayesian audit method that will be tested for the first time in Marion County, Indiana. https://arxiv.org/pdf/1801.00528.pdf

3. Ballot-Polling RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm#

4. Bayesian Audit Tool: http://audits.csail.mit.edu/

5. Comparison RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#

Contact

Jerome Lovato

jlovato@eac.gov

(202)805-4613

Social media

@ Email
listen@eac.gov

Facebook
Facebook.com/eacgov1

Twitter
@EACgov

Youtube Channel
Election Assistance Commission

Website
www.eac.gov

Appendix B

Introduction:

This document reports the results of the RLA pilot conducted in Marion County, Indiana on May 29-30.

Marion County stores ballots by precinct ID (election day voted ballots (P), absentee (A) and unreadable (U)). There may be multiple absentee and/or unreadable batches (groups of ballots) differentiated by timestamps. We did not change this organizational structure for the audit. Rather, we adjusted the ballot manifests.

In the following, section 1 includes the implementation details for the 2016 General Presidential Race, section 2 covers the details for the 2018 Primary Sheriff Race (Democratic) and section 3 covers the details for the 2018 Primary U.S. Senate Race (Republican).

All the methods described below use an input seed (a random number with at least 20 digits). This input seed is used to begin the process of generating random numbers. In our case, this was achieved by rolling a 10-sided die which resulted in the input seed being 66286159831966888996. This input seed was used by Stark's RLA and Rivest's Bayesian method tools to generate a pseudo-random sample[2] of ballots.

The following risk limits (see Appendix A) were used for each audit:

- A Risk Limit of 10% for Stark's method
- A Bayesian Limit of 5% for Rivest's method

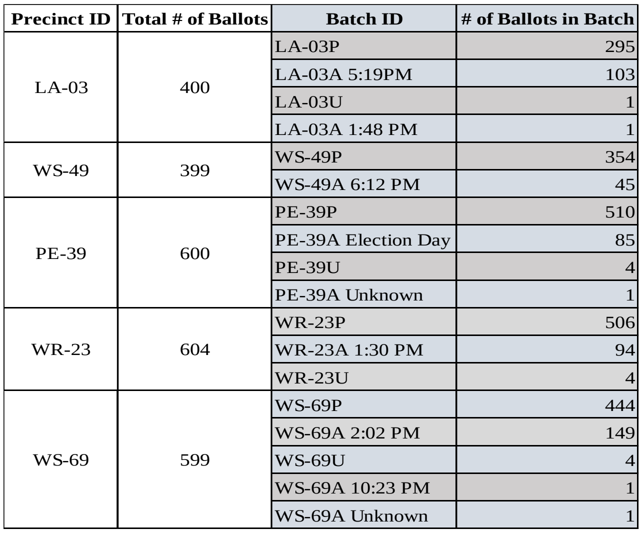
[2] https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Section 1: Risk-Limiting Audit for the 2016 General Presidential Election

For this race, we selected five precincts (LA-03, WS-49, PE-39, WR-23 and WS-69). The candidates were Donald Trump, Hillary Clinton, Gary Johnson and Write-In. Ballot Polling was employed with two approaches (Stark's RLA and Rivest's Bayesian). The ballot polling procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Results for each ballot were tallied

Creating Manifest:



Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
LA-03	400	LA-03P	295
		LA-03A 5:19PM	103
		LA-03U	1
		LA-03A 1:48 PM	1
WS-49	399	WS-49P	354
		WS-49A 6:12 PM	45
PE-39	600	PE-39P	510
		PE-39A Election Day	85
		PE-39U	4
		PE-39A Unknown	1
WR-23	604	WR-23P	506
		WR-23A 1:30 PM	94
		WR-23U	4
WS-69	599	WS-69P	444
		WS-69A 2:02 PM	149
		WS-69U	4
		WS-69A 10:23 PM	1
		WS-69A Unknown	1

Table 1: Manifest

Converting manifest to tool-readable format:

We copied and pasted the fields ("Batch ID (include timestamp if available)","# Ballots") into a notepad file.

Example:

Precinct: LA-03
"Batch ID (include timestamp if available)","#Ballots"
LA-03P, 295

Absentee Ballots:
"Batch ID (include timestamp if available)","#Ballots"
LA-03A 5:19 PM,103

Unreadable Ballots:
"Batch ID (include timestamp if available)","#Ballots"
LA-03U,1

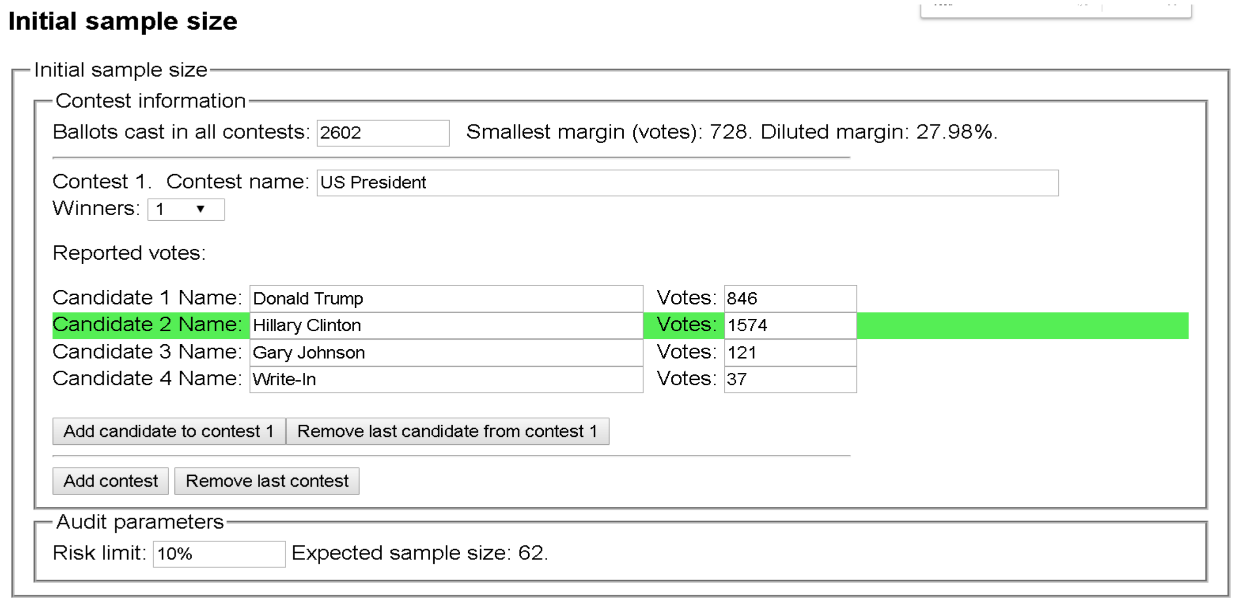
Output:

```
LA-03P,295
LA-03A 5:19 PM,103
LA-03A 1:48 PM,1
LA-03U,1
WS-49P,354
WS-49A 6:12PM,45
PE-39P,510
PE-39A Election Day,85
PE-39U,4
PE-39A Unknown,1
WR-23P,506
WR-23A 1:30 PM,94
WR-23U,4
WS-69P,444
WS-69A 2:02 PM,149
WS-69U,4
WS-69A 10:23 PM,1
WS-69A Unknown,1
```

Implementation:

Ballot Polling (Stark RLA Method):

The above fields were input into the tool https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm# The sample size of ballots was calculated by entering reported votes by candidate and total number of votes cast. Here the sample size was 62.



Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: 2602 Smallest margin (votes): 728. Diluted margin: 27.98%.

Contest 1. Contest name: US President

Winners: 1 ▾

Reported votes:

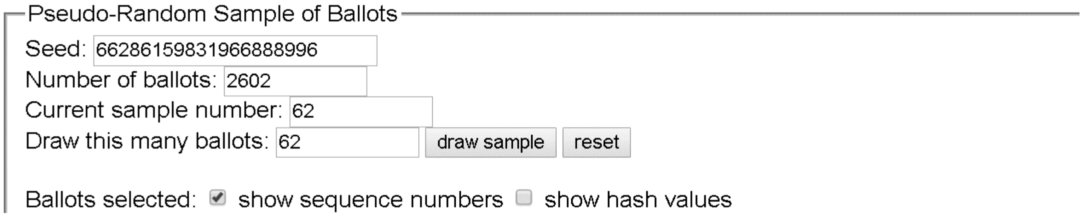
Candidate 1 Name:	Donald Trump	Votes:	846
Candidate 2 Name:	Hillary Clinton	Votes:	1574
Candidate 3 Name:	Gary Johnson	Votes:	121
Candidate 4 Name:	Write-In	Votes:	37

Add candidate to contest 1
Remove last candidate from contest 1
Add contest
Remove last contest

Audit parameters

Risk limit: 10% Expected sample size: 62.

The seed number was input into the tool in order to generate a pseudo-random sample of ballots. The ‘current sample number’ field was initialized to 0. The fields ‘Number of ballots’ and ‘Draw this many ballots' are auto-initialized. The random ballot numbers were selected and sorted with duplicates removed when the draw sample button was clicked. In our case, 61 ballots were selected after removing duplicates.



Pseudo-Random Sample of Ballots

Seed: 66286159831966888996

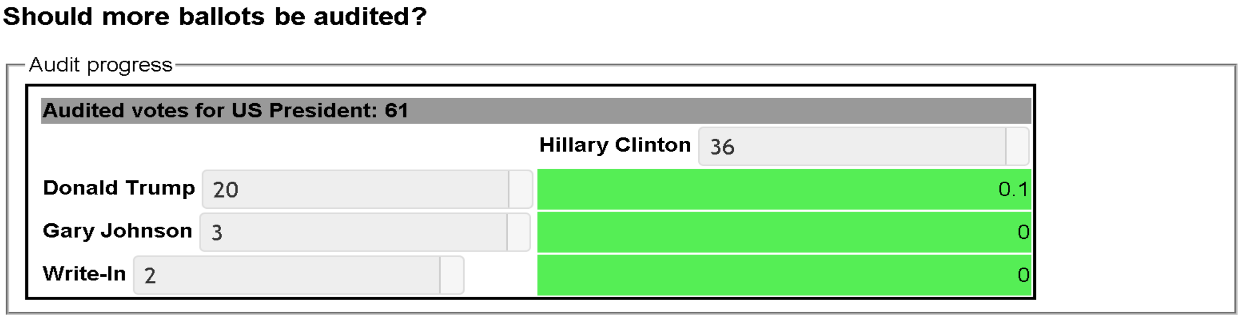
Number of ballots: 2602

Current sample number: 62

Draw this many ballots: 62

Ballots selected: ☑ show sequence numbers □ show hash values

The sorted sample ballots were examined by hand (audited) with the results as shown below:



Should more ballots be audited?

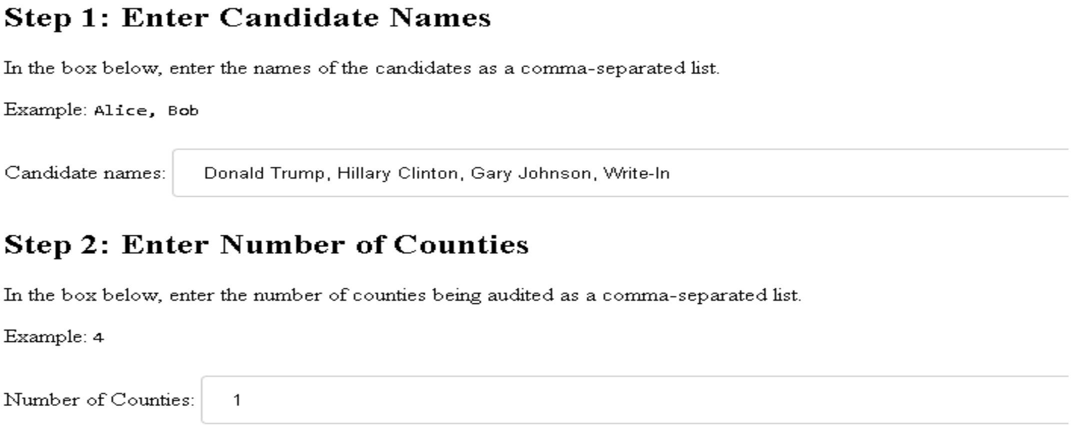
Audit progress

Audited votes for US President: 61

	Hillary Clinton	36
Donald Trump	20	0.1
Gary Johnson	3	0
Write-In	2	0

Bayesian Method (Rivest's Method):

The Bayesian tool was initialized with the following fields:



Step 1: Enter Candidate Names

In the box below, enter the names of the candidates as a comma-separated list.

Example: `Alice, Bob`

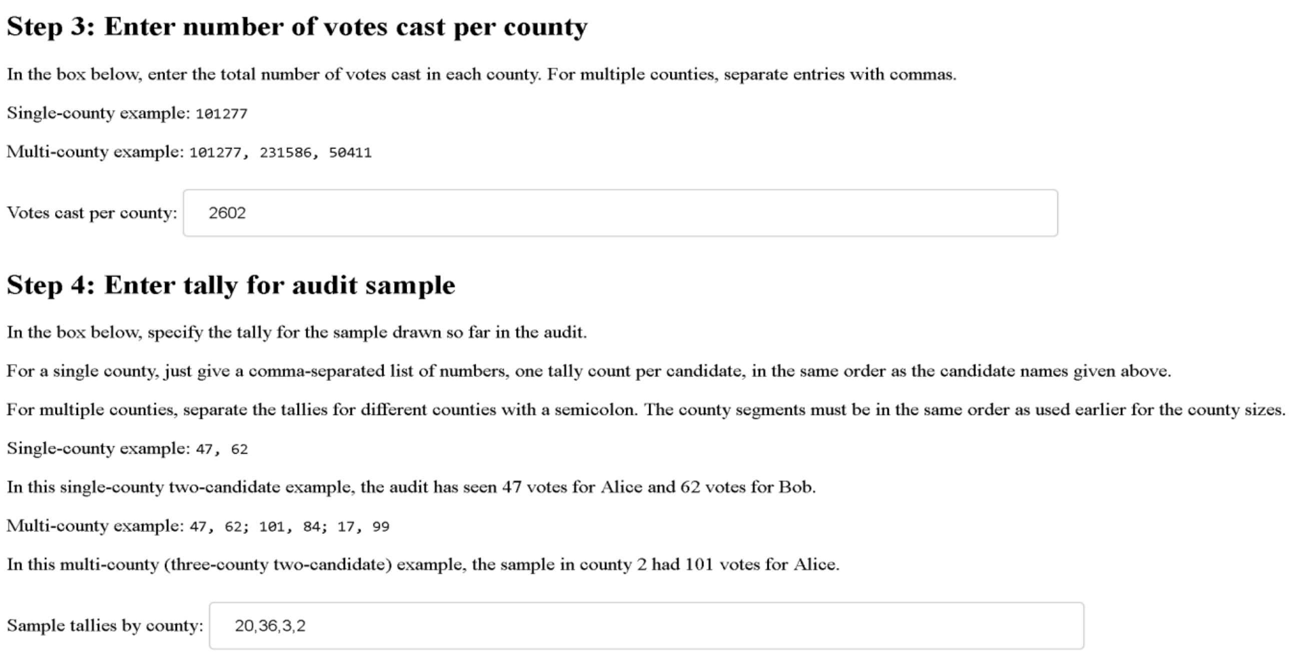
Candidate names: Donald Trump, Hillary Clinton, Gary Johnson, Write-In

Step 2: Enter Number of Counties

In the box below, enter the number of counties being audited as a comma-separated list.

Example: 4

Number of Counties: 1



Step 3: Enter number of votes cast per county

In the box below, enter the total number of votes cast in each county. For multiple counties, separate entries with commas.

Single-county example: `101277`

Multi-county example: `101277, 231586, 50411`

Votes cast per county: 2602

Step 4: Enter tally for audit sample

In the box below, specify the tally for the sample drawn so far in the audit.

For a single county, just give a comma-separated list of numbers, one tally count per candidate, in the same order as the candidate names given above.

For multiple counties, separate the tallies for different counties with a semicolon. The county segments must be in the same order as used earlier for the county sizes.

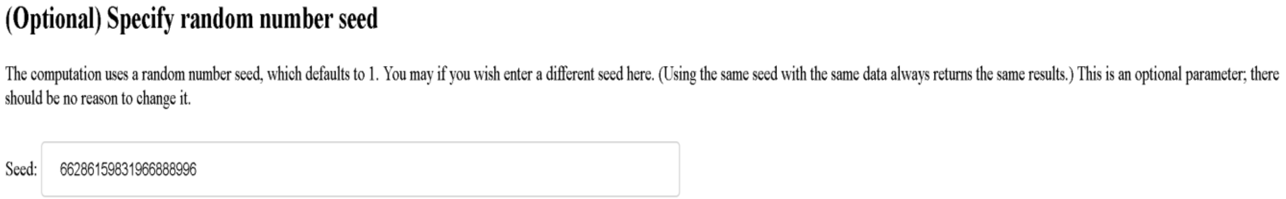
Single-county example: `47, 62`

In this single-county two-candidate example, the audit has seen 47 votes for Alice and 62 votes for Bob.

Multi-county example: `47, 62; 101, 84; 17, 99`

In this multi-county (three-county two-candidate) example, the sample in county 2 had 101 votes for Alice.

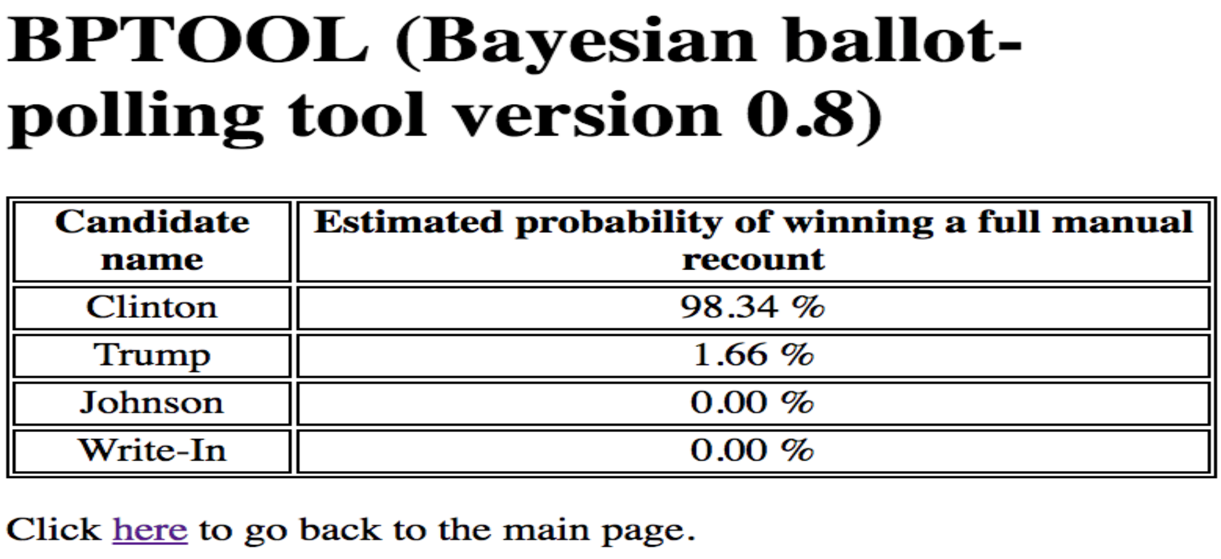
Sample tallies by county: 20,36,3,2



(Optional) Specify random number seed

The computation uses a random number seed, which defaults to 1. You may if you wish enter a different seed here. (Using the same seed with the same data always returns the same results.) This is an optional parameter; there should be no reason to change it.

Seed: 66286159831966888996



BPTOOL (Bayesian ballot-polling tool version 0.8)

Candidate name	Estimated probability of winning a full manual recount
Clinton	98.34 %
Trump	1.66 %
Johnson	0.00 %
Write-In	0.00 %

Click here to go back to the main page.

After auditing 61 ballots, Stark’s tool and the BP Tool reached the risk limits of 10% and 5%. This estimated the probability of Hillary Clinton winning the race without a full manual recount.

Section 2: Risk-Limiting Audit for the 2018 Primary Sheriff Election (Democratic)

For this race, we selected ten precincts (PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27). The candidates were Bill Benjamin, Kerry Joseph Forestal and Undervote (for an RLA). The ballot selections were made using a combination of a Three-Cut and random sampling method. The Ballot Polling audit was conducted using two approaches (Stark's RLA and Rivest's Bayesian). The ballot polling procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Results for each ballot were tallied

Creating Manifest:

Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
PI-09	198	PI-09P	189
		PI-09A 9:34 PM	9
		PI-09U	0
WR-35	195	WR-35P	184
		WR-35A 3:54 PM	11
WR-33	195	WR-33A 7:12 PM	1
		WR-33U	1
		WR-33P	181
		WR-33A 4:07 PM	12
PI-19	186	PI-19P	178
		PI-19A 5:04 PM	7
		PI-19U	1
PI-13	183	PI-13P	80
		PI-13A (A) A	27
		PI-13A (B) B	9
		PI-13A (C) C	25
		PI-13A (D) D	12
		PI-13A (E) E	8
		PI-13A (F) F	20
		PI-13U	2
WS-27	168	WS-27P	147
		WS-27A 3:40PM	21
WR-28	166	WR-28P	158
		WR-28A 1:10PM	8
PI-08	154	PI-08P	147
		PI-08A 9:50 PM	7
WS-14	154	WS-14P	134
		WS-14A 4:37 PM	20
LA-18	148	LA-18P	136
		LA-18A Unknown	12

Table 2: Manifest

Converting Table 2 to tool-readable format:

We copied and pasted the fields (“Batch ID (include timestamp if available)”,”# Ballots”) into a notepad file.

Example:

```
Precinct: PI-09
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09P,189

Absentee Ballots:
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09A 9:34 PM,9

Unreadable Ballots:
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09U,0
```

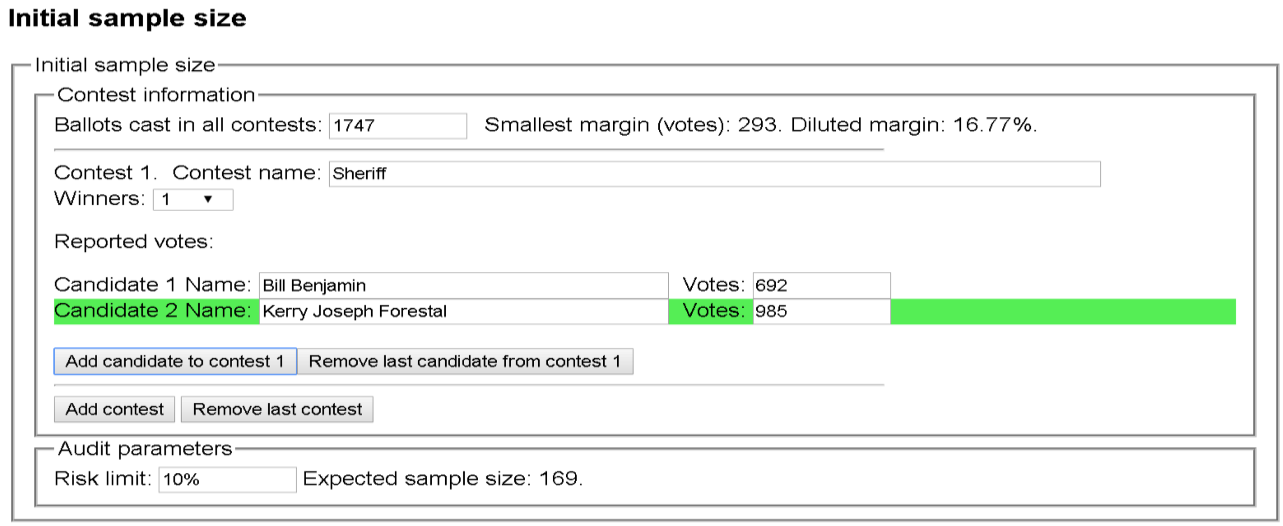
Output:

```
PI-09P,189
PI-09A 9:34 PM,9
PI-09U,0
WR-35P,184
WR-35A 3:54 PM,11
WR-33A 7:12 PM,1
WR-33U,1
WR-33P,181
WR-33A 4:07 PM,12
PI-19P,178
PI-19A 5:04 PM,7
PI-19U,1
PI-13P,80
PI-13A (A) A,27
PI-13A (B) B,9
PI-13A (C) C,25
PI-13A (D) D,12
PI-13A (E) E,8
PI-13A (F) F,20
PI-13U,2
WS-27P,147
WS-27A 3:40PM,21
WR-28P,158
WR-28A 1:10PM,8
PI-08P,147
PI-08A 9:50 PM,7
WS-14P,134
WS-14A 4:37 PM,20
LA-18P,136
LA-18A Unknown,12
```

Implementation:

Ballot Polling: (Stark RLA Method)

The above fields were input into the tool https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm# The sample size of ballots was calculated by entering reported votes by candidate and total number of votes cast. Here the sample size was 169.



Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: 1747 Smallest margin (votes): 293. Diluted margin: 16.77%.

Contest 1. Contest name: Sheriff

Winners: 1

Reported votes:

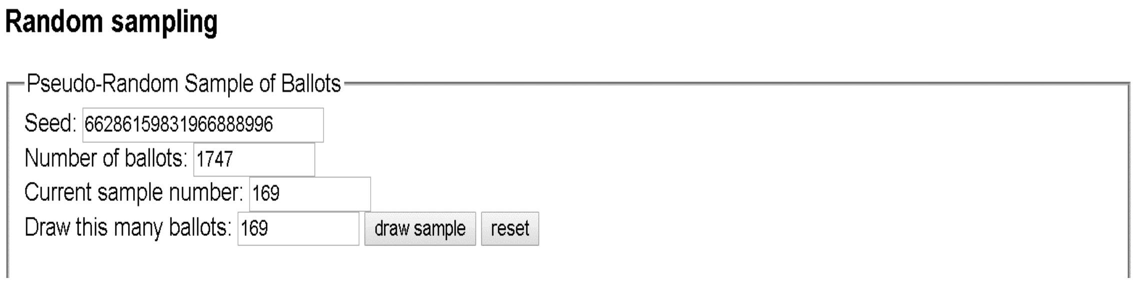
Candidate 1 Name:	Bill Benjamin	Votes:	692
Candidate 2 Name:	Kerry Joseph Forestal	Votes:	985

Audit parameters

Risk limit: 10% Expected sample size: 169.

Add candidate to contest 1
Remove last candidate from contest 1
Add contest
Remove last contest

The seed number was input into the tool in order to generate a pseudo-random sample of ballots. The 'current sample number' field was initialized to 0. The fields 'Number of ballots' and 'Draw this many ballots' are auto-initialized. The random ballot numbers were selected and sorted with duplicates removed when the draw sample button was clicked. In our case, 155 ballots were selected after removing duplicates.



Random sampling

Pseudo-Random Sample of Ballots

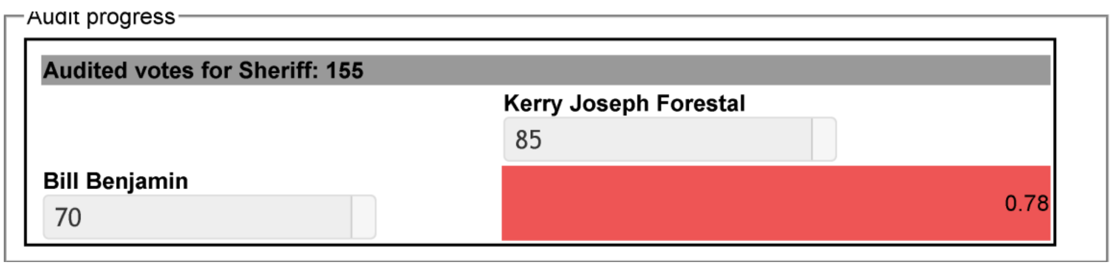
Seed: 6628615983196688896

Number of ballots: 1747

Current sample number: 169

Draw this many ballots: 169

The sorted sample ballots were examined by hand (audited) with the results as shown below:



Audit progress

Audited votes for Sheriff: 155

Kerry Joseph Forestal

85

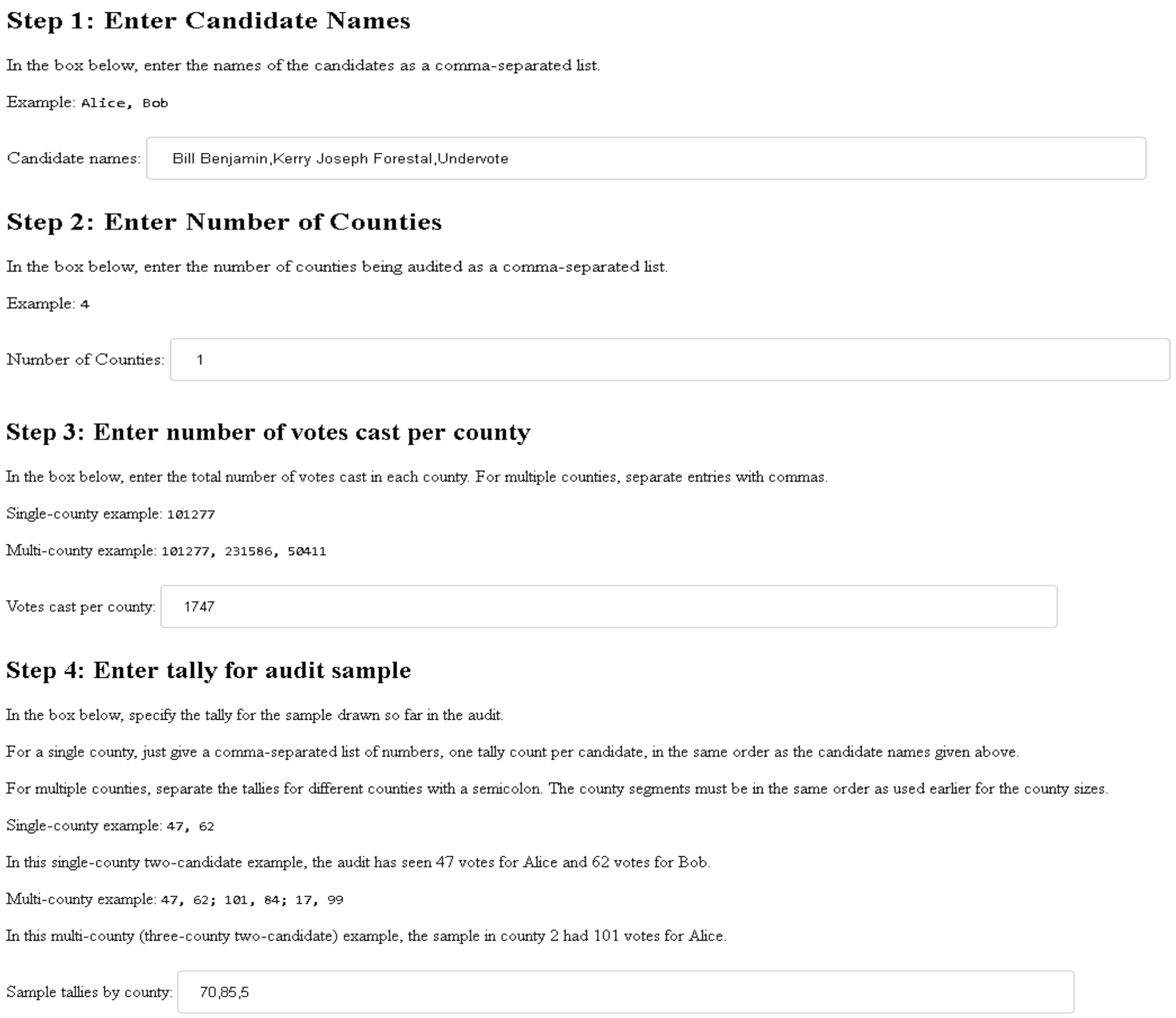
Bill Benjamin

70

Once one has reached the sample number of ballots, if the risk limit is not met one continues the selection of ballots, using the three-cut method until the risk limit has been reached. In this case,13 more ballots were needed for Kerry Joseph Forestal to meet the risk limit.

Bayesian Method: (Rivest's Method)

The Bayesian tool was initialized with the following fields:



Step 1: Enter Candidate Names

In the box below, enter the names of the candidates as a comma-separated list.

Example: `Alice, Bob`

Candidate names: Bill Benjamin,Kerry Joseph Forestal,Undervote

Step 2: Enter Number of Counties

In the box below, enter the number of counties being audited as a comma-separated list.

Example: `4`

Number of Counties: 1

Step 3: Enter number of votes cast per county

In the box below, enter the total number of votes cast in each county. For multiple counties, separate entries with commas.

Single-county example: `101277`

Multi-county example: `101277, 231586, 50411`

Votes cast per county: 1747

Step 4: Enter tally for audit sample

In the box below, specify the tally for the sample drawn so far in the audit.

For a single county, just give a comma-separated list of numbers, one tally count per candidate, in the same order as the candidate names given above.

For multiple counties, separate the tallies for different counties with a semicolon. The county segments must be in the same order as used earlier for the county sizes.

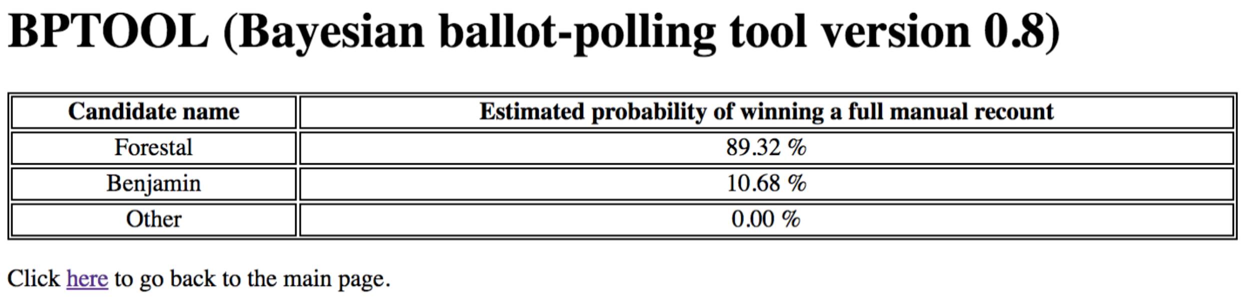
Single-county example: `47, 62`

In this single-county two-candidate example, the audit has seen 47 votes for Alice and 62 votes for Bob.

Multi-county example: `47, 62; 101, 84; 17, 99`

In this multi-county (three-county two-candidate) example, the sample in county 2 had 101 votes for Alice.

Sample tallies by county: 70,85,5



BPTOOL (Bayesian ballot-polling tool version 0.8)

Candidate name	Estimated probability of winning a full manual recount
Forestal	89.32 %
Benjamin	10.68 %
Other	0.00 %

Click here to go back to the main page.

Once one has reached the sample number of ballots, if the Bayesian limit is not met one continues the selection of ballots, using the three-cut method until the Bayesian limit has been reached. In this case,10 more ballots were needed for Kerry Joseph Forestal to meet the Bayesian limit.

Section 3: Risk-Limiting Audit for 2018 Primary U.S. Senate Election (Republican)

For this race, we selected ten precincts (PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27). The candidates were Mike Braun, Luke Messer, Todd Rokita and Other (includes undervotes and overvotes). A ballot comparison was employed for this race. This procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Compare each ballot to its simulated cast vote record (CVR)

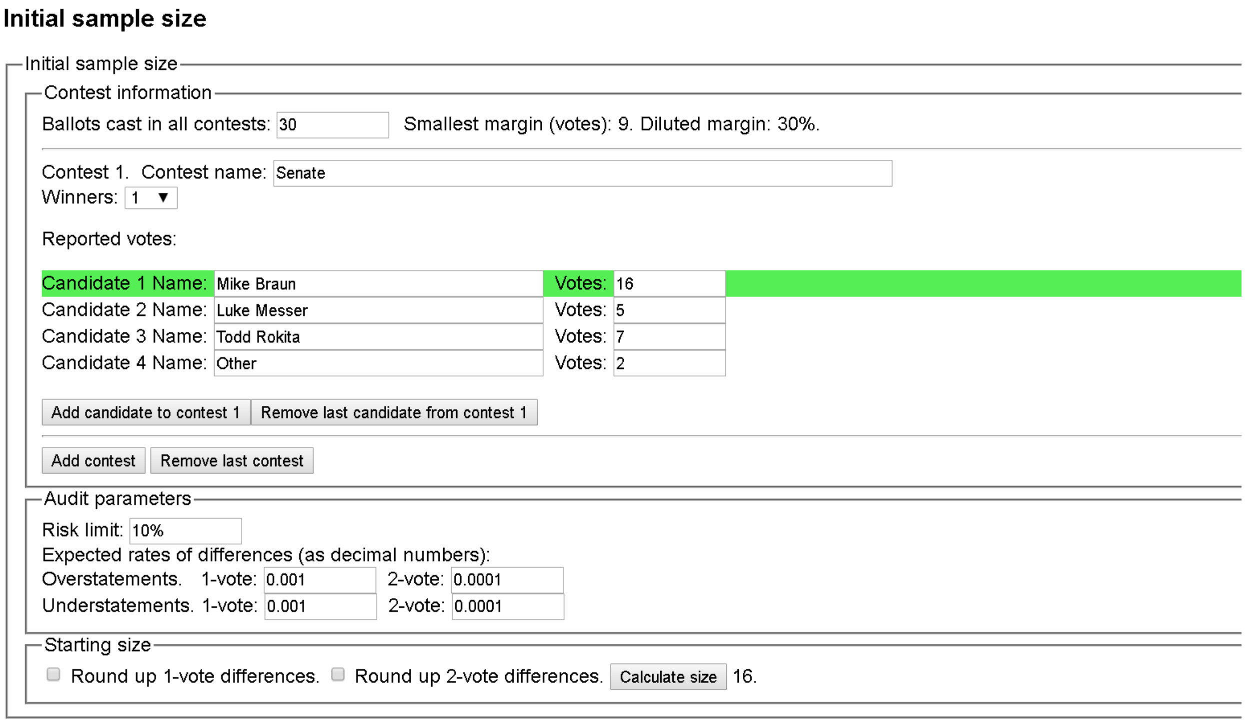
Creating Manifest:

Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
PI-09	156	PI-09P	152
		PI-09A 9:34 PM	4
WR-35	169	WR-35P	162
		WR-35A 3:54 PM	7
WR-33	127	WR-33P	118
		WR-33A 4:07 PM	9
PI-19	120	PI-19P	113
		PI-19A 5:04 PM	7
PI-13	197	PI-13P	52
		PI-13A (a) a	25
		PI-13A (b) b	21
		PI-13A (c) c	26
		PI-13A (d) d	28
		PI-13A (e) e	12
		PI-13A (f) f	31
		PI-13U	2
WS-27	141	WS-27P	126
		WS-27A 3:54 PM	15
WR-28	124	WR-28P	122
		WR-28A 1:10 PM	2
PI-08	170	PI-08P	155
		PI-08A 9:50 PM	15
WS-14	167	WS-14P	154
		WS-14A 4:37 PM	12
		WS-14U	1
LA-18	119	LA-18P	114
		LA-18A Unknown	5

Table 3: Manifest

Implementation:

The total number of ballots for this race was 1,490. However, due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method.


Add candidate to contest 1
Remove last candidate from contest 1
Add contest
Remove last contest
Calculate size

Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: 30 Smallest margin (votes): 9. Diluted margin: 30%.

Contest 1. Contest name: Senate
Winners: 1 ▼

Reported votes:

Candidate 1 Name:	Mike Braun	Votes:	16
Candidate 2 Name:	Luke Messer	Votes:	5
Candidate 3 Name:	Todd Rokita	Votes:	7
Candidate 4 Name:	Other	Votes:	2

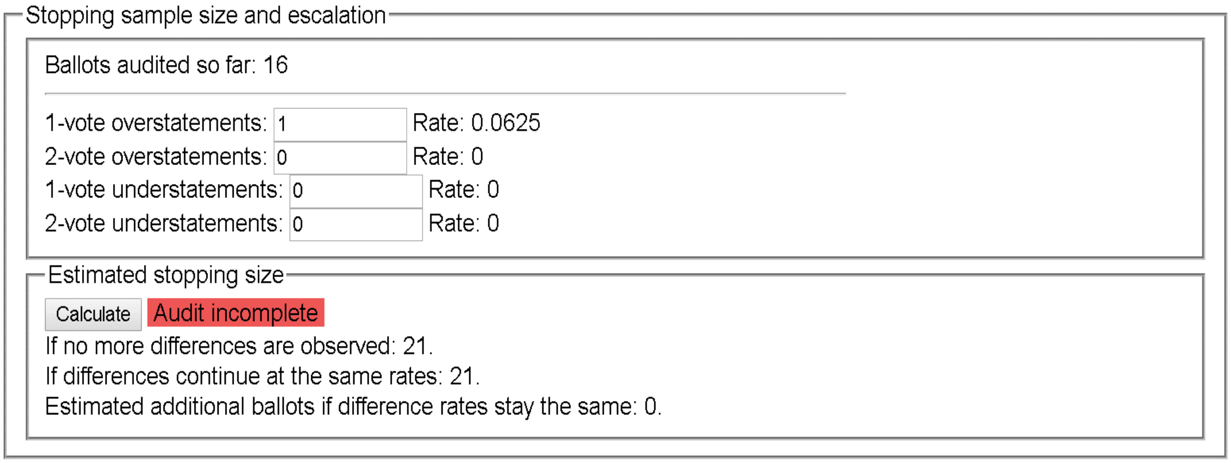
Audit parameters

Risk limit: 10%
Expected rates of differences (as decimal numbers):
Overstatements. 1-vote: 0.001 2-vote: 0.0001
Understatements. 1-vote: 0.001 2-vote: 0.0001

Starting size

□ Round up 1-vote differences. □ Round up 2-vote differences. Calculate size 16.

Output:



Stopping sample size and escalation

Ballots audited so far: 16

1-vote overstatements: 1 Rate: 0.0625
2-vote overstatements: 0 Rate: 0
1-vote understatements: 0 Rate: 0
2-vote understatements: 0 Rate: 0

Estimated stopping size

Calculate Audit incomplete
If no more differences are observed: 21.
If differences continue at the same rates: 21.
Estimated additional ballots if difference rates stay the same: 0.

According to the algorithm, at least 21 more ballots would need to be selected before it met the risk limit. This led to an effective recount of the 30 ballots in our full population of ballots. The recount did not contradict the certified outcome.

Conclusions:

For the 2016 Presidential race, after auditing sample ballots, the Stark's tool and the BP Tool reached the risk limits of 10% and 5%. This estimated the probability of Hillary Clinton winning the race without a full manual recount.

For the 2018 Primary Democrat Sheriff race, after auditing sample ballots, the Stark's tool and the BP Tool failed to reach the risk limits. In this case, 13 more ballots for Stark's tool and 10 more ballots for BP tool were needed to verify Kerry Joseph Forestal as a winner. However, these audits were ceased early due to time constraints.

For the 2018 Primary Republican U.S. Senator race, simulated CVRs were used for comparison. Due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method. The audit ceased early but did not contradict the election outcome for Mike Braun as the winner.

VSTOP

Appendix C

Observation of Denver County Primary 2018 Risk-Limiting Audit (RLA)

By Jessica Martin, Voting System Technical Oversight Program (VSTOP), Project Manager

Risk Limiting Audits (RLAs) are becoming more popular in Election Administration and in some States they are now legally required. As a former Election Coordinator in a county that prevalently used DRE (Direct Recording Electronic) devices, I had a lot of trepidation and questions about the trending usage of RLAs. Below is my report of what I learned from attending the RLA for the June 26, 2018 Primary Election in the State of Colorado.

When I arrived on Thursday July 5th, I was expecting to see a flurry of activity as 9:00am – 5:00pm was listed as wrapping up the tabulation of ballots, organizing/storage of ballots and county data entry into the state RLA tool. However, the bulk of this work had already been done and the County of Denver had graciously left a few items over so they could demonstrate this process from 4:00pm – 5:00pm to benefit those of us who had traveled for this event. The state requires that all ballot manifest information be entered in the RLA tool the evening before the audit seed is selected.

Colorado has 64 counties and the only counties which did not participate in the Primary RLA were the three counties that tabulated their results by hand. On Friday July 6th, at 9:00am the Secretary of State held a public meeting where he (and a number of volunteers) rolled a 10 sided die a total of 20 times to create the random seed. By 9:36am all Counties were able to go directly to the tool to see which ballots had been selected. In addition, counties receive an email with this information. From this time until the ballot selection occurred, the County was conducting work behind the scenes to ensure that ballot pulling would go off without a hitch. Unfortunately, much of this I did not get to see, but I thought it was important to note that each box of ballots was labeled with which ballots needed to be retrieved to ensure that teams retrieve those ballots in a single visit to the box. Copies of actual ballots were left as place markers.

The majority of counties, including Denver County where I visited, completed a comparison audit. A comparison audit requires that the County's voting system have the ability to organize and disseminate case vote records (CVR) appropriately. In contrast, when we did the Marion County, Indiana RLA they were not sure of the process and tools needed to connect the EVS 5.2.0.0 marked ballots and CVRs without contacting the vendor for assistance. In Denver County the ballots are imprinted with their corresponding CVR. An image of the imprint number on a copy of the ballot can be seen below (see Image 1). Although imprinting isn't the only method to connect the ballot to the corresponding CVR, being able to tie the ballot with the correct CVR is a necessity for a comparison RLA.

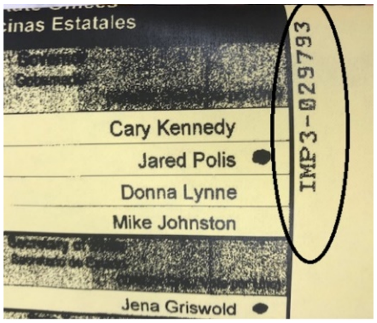


Image 1

After an election, the Secretary of State selects two races for each County (one statewide and one countywide) and then also determines the risk limit. This year the risk limit for comparison audits was 5% and the ballot polling risk limit was 10%. When asked which races are selected, it was noted that if the County Clerk and Secretary of State race are on the ballot then they are typically chosen.

When a ballot is pulled from a batch to be audited, a photocopy of the ballot image is left in its place. The pulling of ballots is an activity that involved multiple bipartisan teams of two, who would seal and unseal boxes and search through folders within those boxes. In addition, this all occurs in a secure room that is under video surveillance. The pulling of ballots is very methodical and organized. In the rare case a ballot is not found, the process is to enter into the RLA tool that the ballot was not found and the software treats this as a fail.

Once all of the ballots had been pulled a bipartisan team of one Republican Judge and one Democrat Judge confirmed every ballot was entered correctly into the tool. If there is a question about how a ballot was marked, there is an adjudication reference guide (see Image 2) that can be used to resolve the question. If the judges still disagree on a vote there is an option for "no consent."

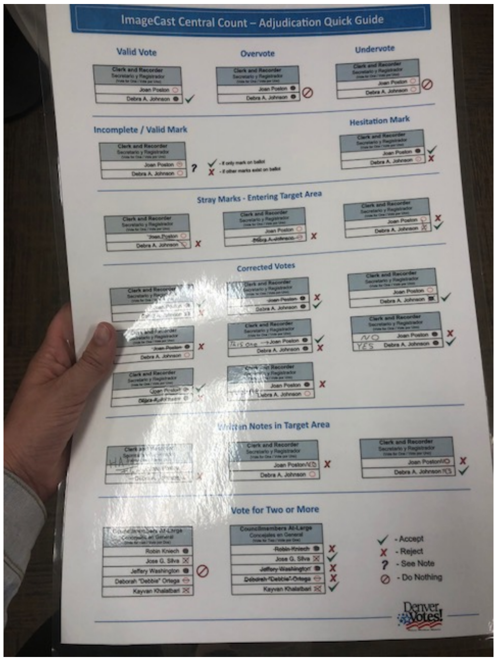


Image 2

Although only two races were chosen to be audited, all of the races voted on in the selected ballot are entered into the tool that collects the results of each ballot. The reason behind this is to collect as much data as possible.

The entry of data in the RLA tool appeared to be the most time consuming portion as we only had one person entering the data and one team of judges confirming that it was correct. Nonetheless, it was a very efficient process and was completed in the timeline allotted by the Office of the Secretary of State. If the first round of the ballot comparison audit had not met the risk limit, Denver County would have gone onto a second round. In this case, a second round of auditing was not needed and Denver County successfully completed the audit.

My observation of the RLA in Denver County alleviated my fears regarding ballot security, disorganization and undue administrative burden on the County that I previously had. I appreciated the opportunity to see Denver County's RLA, and I feel much more prepared to manage an RLA project in the future if appropriate. I saw a lot of similarities and differences between our pilot RLA in Marion County and Denver County's Primary 2018 RLA. The main difference is that much of Colorado's activities were automated and with software tools, whereas for Marion County a lot of our work was done manually via excel. Another difference was some of the laws currently in Colorado around conducting RLA's and canvassing dates and that ballots are open records.

Schedule of Events

COLORADO RISK-LIMITING AUDIT – 2018 PRIMARY ELECTION		
Day/date	**Events**	**Location**
Thursday, July 5th 9am – 5pm (est.)	• Counties finish tabulating ballots, enabling observers to watch how county officials organize and store paper ballots for retrieval during RLA • Counties export, hash and upload ballot manifests and cast vote record (CVR) files to Secretary of State via RLA software tool	Denver Elections Division 200 West 14th Avenue, Ste. 100 Denver, CO 80204
Friday, July 6th 9 am – 12 pm	• Secretary of State convenes a public meeting to establish 20-digit random seed by sequential rolls of 10-sided dice; the random seed is then utilized in the RLA software's pseudo-random number generator (PRNG) to randomly select ballots in each county for examination during the RLA • After public meeting adjourns, Secretary of State staff will demonstrate for observers how each county's audit is defined and launched using the RLA software	Colorado Secretary of State 1700 Broadway, 3rd Floor Denver, CO 80290
Friday, July 6th (afternoon) 2 pm – 5 pm (est.)	• Once the Secretary of State defines and starts each county's audit, the RLA software generates a list of ballots that each county audit board must examine • Each county downloads the list of randomly selected ballots, and bipartisan teams of election judges then locate and retrieve those specific ballots from storage containers	Denver Elections Division
Saturday, July 7th 9:00 am – 12:00 pm (est.)	• Bipartisan county audit boards begin the audit in earnest, and report voter markings from randomly selected ballots into RLA software • At conclusion of first round, RLA software compares the audit boards' reports to the corresponding cast vote record (CVR) for each audited ballot. • RLA software identifies any discrepancies between human and machine tabulations, and determines whether the risk limit is satisfied or an additional round of auditing is required.	Denver Elections Division

Resource

Audit Center Colorado Secretary of State by Wayne Williams
https://www.sos.state.co.us/pubs/elections/auditCenter.html

Acknowledgement

My gracious hosts at the Colorado Secretary of State Office and Denver County Elections Division who answered my abundant list of questions, sometimes before I even asked them.