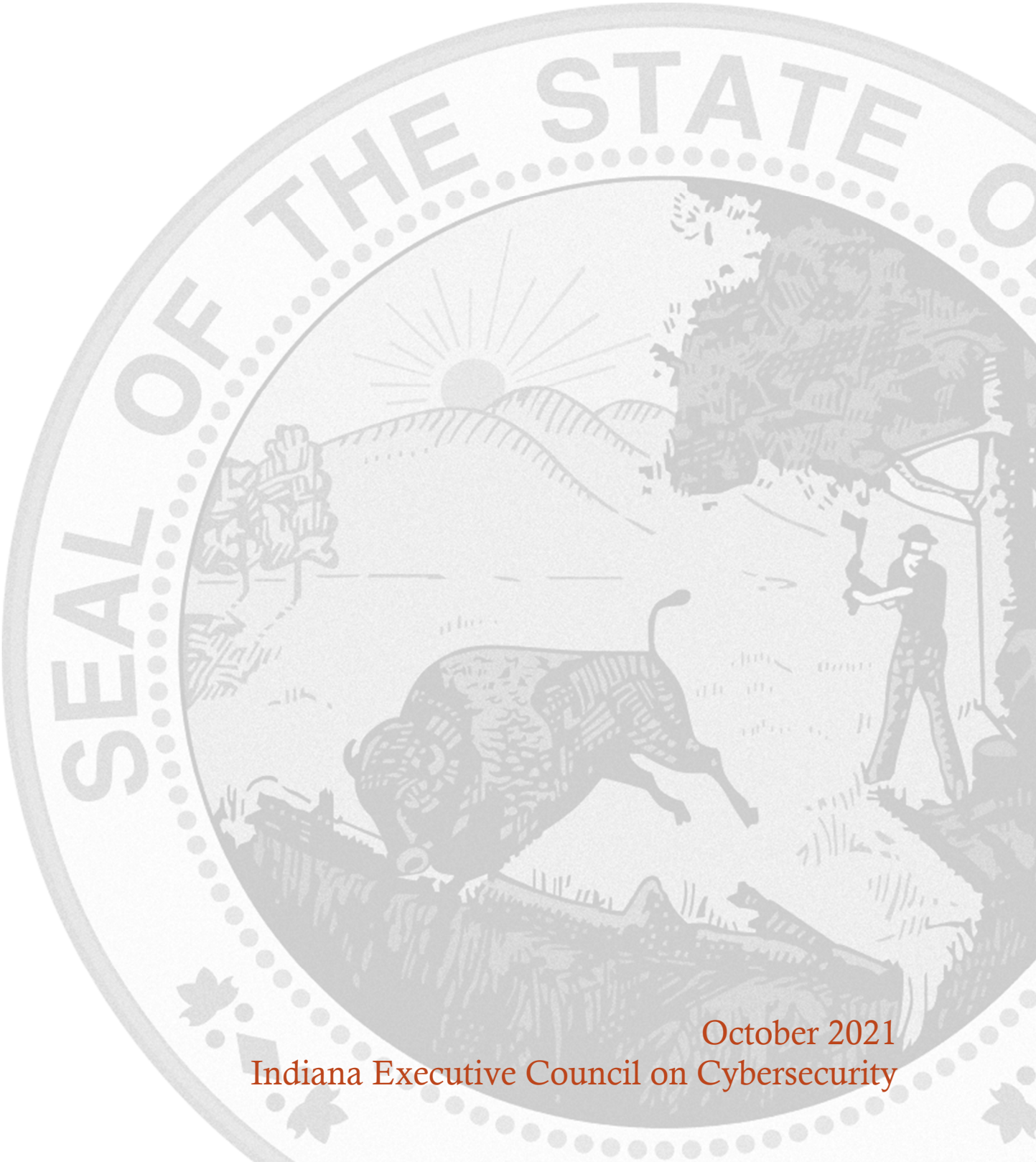
ELECTION COMMITTEE STRATEGIC PLAN

Chair: Secretary Holli Sullivan
Co-Chair: Beth Dlug



October 2021
Indiana Executive Council on Cybersecurity

Election Committee Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organization Title	Member Type
Bagga	Jay	Ball State University VSTOP	Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Computer Science	Full Time
Bailey	Gerry	Corvano LLC	President	As Needed
Bonnet	Jerry	Indiana Secretary of State	General Counsel	As Needed
Byers	Bryan	Ball State University VSTOP	Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Criminal Justice and Criminology	As Needed
Cooper	Seth	Baker Tilly	Project Manager	As Needed
Dlug	Beth	Allen County Election Board	Elections Director	Co-Chair
Fahey	Sean	CIVIX (PCC)	Elections and Campaigns	As Needed
Frank	Michael	Anderson University	Professor of Political Science	As Needed
Herzog	Laura	Hendricks County	Elections Supervisor	Full Time
Hoffmeyer	Rachel	Indiana Secretary of State	Deputy Secretary of State	Full Time Chair Designee-Proxy
King	Brad	Indiana Election Division	Election Division Co-Director	Full Time
Kochevar	Matthew	Indiana Election Division	Co-General Counsel	As Needed

Mays	Lindsey	Indiana Secretary of State	IT Director	As Needed
Nussmeyer	Angela	Indiana Election Division	Election Division Co-Director	Full Time
Sullivan	Holli	Indiana Secretary of State	Secretary of State	Chair
Welch	Von	Indiana University	Associate Vice President for Information Security	As Needed

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

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 (Revised July 2021)**
  - **Collaboration with Federal and Sector Communities of Interest**
    Since the heightened concern over election interference in 2016 and federal designation of Elections as Critical Infrastructure in 2017, communities of interest have come together to provide a significant level of resources focused on election security. The Secretary of State may engage in election cybersecurity collaboration with the following allied organizations:
    - DHS, DOD, US Cyber Command
    - Center for Internet Security
    - Election Infrastructure Information Sharing and Analysis Center
    - MS-Election -ISAC
    - Cybersecurity and Infrastructure Security Agency Election Security Initiative

[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.

- National Association of Secretaries of State
- National Association of State Election Directors
- U. S. Election Assistance Commission (EAC)
- Indiana Fusion Center
- Indiana Executive Council on Cybersecurity
- Association of the Clerks of the Circuit Courts of Indiana
- Indiana Statewide Voter Registration System Core Team
- Indiana Voting System Technical Oversight Program (VSTOP)
- Indiana Voter Registration Association
- EAC accredited Voting System Testing Labs (VSTLs)
- Association of Government IT Leaders (GMIS.org)

- **Integration of Cybersecurity Professionalism, Awareness and Practice**
  - The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration.
  - State and local election officials and administrators will be encouraged to engage Certified Information Security Professionals, and provide ongoing cybersecurity awareness, training, and certification opportunities for staff.
  - The Secretary of State will assist VSTOP with the integration of election cybersecurity into the Election Administration Certificate Program (CEATS).

- **Election Infrastructure Monitoring, Hardening, Testing and Auditing**
  The Secretary of State will promote election infrastructure cyber security monitoring and improvements in the following aspects:
  - Monitoring with the use of state-of-the-art contractors and protocols
  - Hardening via technical and process improvements
  - Voting system and electronic poll book testing and certification protocols, and implementation of paper audit trail voting systems
  - Post-election risk-limiting audit program development, funding, and implementation

- **Public Engagement and Confidence**
  The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence including:
  - Surveying the public about election security and integrity concerns
  - Voter outreach, education, and engagement activities
  - Implementation of absentee voting Internet enabled and assistive technology for blind and print disabled voters

- **Continuity, Coordination, Maintenance of Effort and Oversight**
  To assure the highest level of ongoing election cybersecurity vigilance and effort, the Secretary of State may integrate the IECC Election Committee's day-to-day, and election-to-election responsibilities with the professionally managed Indiana Statewide Voter Registration System Core Team.

• **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 continues 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.

- The Secretary of State and Indiana Election Division have been engaged administering Help America Vote Act (HAVA) Election Security Fund appropriated by Congress in 2018 and 2020 ($16,140,537 for Indiana) and $10,000,000 appropriated by the Indiana General Assembly for election cybersecurity initiatives.
  The 2018 – 2022 Election security initiatives include:

  a) grants to counties for to improve physical security of election equipment
  b) grants to counties to upgrade voting equipment (to include voter verifiable paper trails)
  c) implementation of county level and Statewide Voter Registration System network security monitoring
  d) electronic pollbook hardware and software upgrades
  e) network penetration testing exercises
  f) conducting post-election Risk Limiting Audits to confirm election outcomes.

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 cyber threats. 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).
o. Grants to counties for to improve physical security of election equipment.
p. Grants to counties to upgrade voting equipment (to include voter verifiable paper trails).
q. Implementation of county level and Statewide Voter Registration System network security monitoring
r. Electronic poll book hardware and software upgrades.
s. Network penetration testing exercises.
t. Conducting post-election Risk Limiting Audits to confirm election outcomes.

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 sophisticated domestic or overseas perpetrators.
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 (IoT) 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.**
    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
    b. Year Three- deliverables developed with training programs
    c. Year Five – no successful penetration of election systems or databases essential to conducting elections; overall high level of public confidence in election security and outcomes.

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 inform the public promptly and accurately 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 was developed and launched in time for the November 2018 General Election.
    c. VSTOP 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 administering an election is to be immediately reported to the Secretary of State.
    b. The Secretary of State will communicate the details of the incident to appropriate responding security, 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?

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: Collaboration with State, Federal, and Sector Communities

Deliverable: Collaboration with State, Federal, and Sector Communities

General information

1. **What is the deliverable?**
   a. Collaboration with State, Federal and Sector Communities
      - Since the heightened concern over election interference in 2016 and federal designation of Elections as Critical Infrastructure in 2017, communities of interest have come together to provide a significant level of resources focused on election security. The Secretary of State will continue engage in election cybersecurity collaboration with the following allied organizations:

        - DHS, DOD, US Cyber Command
        - Center for Internet Security
        - Election Infrastructure Information Sharing and Analysis Center
        - MS-Election -ISAC
        - Cybersecurity and Infrastructure Security Agency Election Security Initiative
        - National Association of Secretaries of State
        - National Association of State Election Directors
        - U. S. Election Assistance Commission (EAC)
        - Indiana Fusion Center
        - Indiana Executive Council on Cybersecurity
        - Association of the Clerks of the Circuit Courts of Indiana
        - Indiana Statewide Voter Registration System Core Team
        - Indiana Voting System Technical Oversight Program (VSTOP)
        - Indiana Voter Registration Association
        - EAC accredited Voting System Testing Labs (VSTLs)
        - Association of Government IT Leaders (GMIS.org)

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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?**
   - ☒ 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. Effective leveraging of activity, resources and knowledgebase of a broad and deep community of interest. Efficient exchange of situational awareness and intelligence information.

6. **What metric or measurement will be used to define success?**
   a. Number of organizations collaborating in the effort, number of information and alert exchanges, number of meetings, and activities.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The public; state and local election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Because a number of federal, state, industry and even public organizations are directing resources to election security, the Election Committee recognized the potential for significant overlap. A key aspect of the collaboration effort is to minimize programing overlap, allowing organizations to focus attention and resources on specific, rather than general aspects of election security.

Additional Questions

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

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    - DHS, DOD, US Cyber Command
    - Center for Internet Security

- Election Infrastructure Information Sharing and Analysis Center
- MS-Election -ISAC
- Cybersecurity and Infrastructure Security Agency Election Security Initiative
- National Association of Secretaries of State
- National Association of State Election Directors
- U. S. Election Assistance Commission (EAC)
- Indiana Fusion Center
- Indiana Executive Council on Cybersecurity
- Association of the Clerks of the Circuit Courts of Indiana
- Indiana Statewide Voter Registration System Core Team
- Indiana Voting System Technical Oversight Program (VSTOP)
- Indiana Voter Registration Association
- EAC accredited Voting System Testing Labs (VSTLs)
- Association of Government IT Leaders (GMIS.org)

12. Who should be main lead of this deliverable?

a. The Secretary of State, Indiana Election Division and Statewide Voter Registration System Core Team (SVRS Core Team).

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?

☐ One-time deliverable

☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Establishing collaboration	Secretary of State	100	No Response	
Participation in meetings and exchanges	Secretary of State/Election Division/SVRS Core Team	100	No Response	
Technical monitoring	Secretary of State/Election Division/SVRS Core Team	100	No Response	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
No new resources required.						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Framework for rapid sharing of threat information and rapid response.

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

a. As a result of collaborative effort, focus of resources, and focus of attention, cybersecurity risk should be reduced across the election sector.

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

a. Increased risk of zero-day attack, inefficient utilization of resources due to activity overlap, longer response to threat time.

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

a. Efficiency in utilization of resources, organizational time and effort efficiency, communication of threat and response lead times.

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

☐No ☒ Yes

a. Through the efforts of the National Association of Secretaries of State, many, if not all state election officials are engaging in a collaborative approach to election security.

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?

☒No ☐ Yes

Other Implementation Factors

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

a. Collaboration mitigates inefficiency resulting from duplicative and overlapping efforts. The Committee is not aware of factors that might have a negative impact on collaboration between organizations.

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

☒No ☐ Yes

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

a. Collaboration is expected to be an easily and efficiently sustainable activity.

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

a. See response to question #11 above.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes,

a. Any sector should benefit from collaborative effort.

Communications

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

a. Not applicable because key stakeholders are involved in a collaborative effort.

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

☐No ☒ Yes

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

a. Understanding of the number of organizations, collaborative effort, and resources focused on the effort can help alleviate public concern about election security and serve to dissuade threat actors.

Evaluation Methodology

Objective 1: The new Secretary of State will actively engage with allied organizations indicated in the state's strategic plan by December 31, 2021.

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: The Secretary of State will continue engage in election cybersecurity collaboration with allied organizations every year as appropriate.

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: Integration of Cybersecurity Professionalism, Awareness, and Practice

Deliverable: Integration of Cybersecurity Professionalism, Awareness, and Practice

General Information

1. **What is the deliverable?**
    a. Integration of Cybersecurity Professionalism, Awareness, and Practice

    - The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration.
    - State and local election officials and administrators will be encouraged to engage Certified Information Security Professionals, and provide ongoing cybersecurity awareness, training, and certification opportunities for staff.
    - The Secretary of State will assist VSTOP with the integration of election cybersecurity into the Election Administration Certificate Program (CEATS).

2. **What is the status of this deliverable?**

☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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?**

☒ 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. Integration of experienced, trained and professionally certified cybersecurity resources into all phases of election administration.

6. **What metric or measurement will be used to define success?**
    a. Number of counties (local election administration units) employing, accessing or otherwise utilizing professional cybersecurity resources.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division and Statewide Voter Registration Core Team (SVRS Core Team).

13. **What are the expected challenges to completing this deliverable?**
    a. Possibly local government funding.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Encouragement	Secretary of State, Indiana Election Division, SVRS Core Team	?	N/A	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Local government funding.	Improved, more reliable security outcomes.	Unknown	Unknown	Local Government	State and Federal funding	

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Improved, more reliable election cybersecurity outcomes

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

a. Qualified IT and cyber security professionals will have greater situational awareness, higher and faster threat response capability, improved day-to-day collaboration and maintenance of effort.

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

a. Lower situational awareness, slower threat response and capability, lower day-to-day collaboration, and maintenance of effort.

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

a. Number of counties (local election administration units) employing, accessing or otherwise utilizing professional cybersecurity resources.

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

☐No ☒ Yes

a. Unknown. Possible survey subject.

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?

☐No ☒ Yes

a. Unknown. Possible survey subject.

Other Implementation Factors

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

a. IT and cybersecurity workforce training and workforce limitations.

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

☒No ☐ Yes

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

a. Local government funding for maintenance of effort.

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

a. This deliverable is a topic of discussion within the election sector.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Security outcomes in all sectors would likely be improved through institutionalizing employment of qualified IT and cybersecurity professionals.

Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. Understanding of the utilization of IT and cybersecurity professionals in election administration can help alleviate public concern about election security and serve to dissuade threat actors.

Evaluation Methodology

Objective 1: The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration by November 2024.

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: More than 80 percent of state and local election officials and administrators will provide ongoing cybersecurity awareness, training, and/or certification opportunities by November 2024.

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 Infrastructure Monitoring, Hardening, Testing, and Auditing

Deliverable: Election Infrastructure Monitoring, Hardening, Testing, and Auditing

General Information

1. **What is the deliverable?**
    a. Election Infrastructure Monitoring, Hardening, Testing and Auditing
        - The Secretary of State will promote election infrastructure cyber security monitoring and improvements in the following aspects:
            - Monitoring with the use of state-of-the-art contractors and protocols
            - Hardening via technical and process improvements
            - Voting system and electronic poll book testing and certification protocols, and implementation of paper audit trail voting systems
            - Post-election risk-limiting audit program development, funding, and implementation

2. **What is the status of this deliverable?**
    ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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?**
    ☐ 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. Robust and uniform utilization of technical cyber security products and protocols across state and local election administration platforms and networks.

6. **What metric or measurement will be used to define success?**
    a. A number of counties and election systems, platforms, and networks integrating state-of-the-art cybersecurity tools and monitoring systems.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division, Statewide Voter Registration Core Team (SVRS Core Team).

13. **What are the expected challenges to completing this deliverable?**
    a. Local government funding.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Awareness	Secretary of State, Indiana Election Division, SVRS Core Team	75	05/01/2024	
Implementation	Secretary of State, Indiana Election Division, SVRS Core Team	75	05/01/2024	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
The Secretary of State and Election Division are providing tools and services to counties with federal and state funding.	Additional resources are nor needed at this time.	No Response	No Response	No Response	No Response	

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Higher level of IT and cybersecurity through uniform, proactive deployment of state-of-the-art security and monitoring tools and services.

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

a. Proactive investment in deterrence, early detection and fast response tools, and monitoring will likely be less costly and more supportive of public confidence than after-the-fact responses to security breaches.

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

a. Higher degree of sector network and infrastructure vulnerability, longer detection and response times, lower public confidence in election efficiency and outcomes.

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

a. Number of counties, election platforms, and networks utilizing the tools and monitoring services

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

☐No ☒ Yes

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?

☐No ☒ Yes

Other Implementation Factors

---

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

a. Local government units and IT administrator evaluation, approval, implementation, and collaboration.

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

☒No ☐ Yes

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

a. Sustained collaboration with local government and county election officials and administrators, sustained funding.

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

a. Active engagement on implementation of this deliverable across the election sector is ongoing.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors utilizing IT platforms and networks would likely benefit from utilization of state-of-the-art security tools and monitoring services.

Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. Understanding of the utilization of state-of-the-art security tools and monitoring services in election administration can help alleviate public concern about election security and serve to dissuade threat actors.

Evaluation Methodology

Objective 1: The Secretary of State will promote election infrastructure monitoring, hardening, testing, and auditing improvements every year until December 2024.

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: Public Engagement and Confidence

Deliverable: Public Engagement and Confidence

General Information

1. **What is the deliverable?**
    a. Public Engagement and Confidence
        - The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence including:
            - Surveying the public about election security and integrity concerns
            - Voter outreach, education, and engagement activities
            - Implementation of Internet enabled absentee voting and assistive technology for blind and print disabled voters

2. **What is the status of this deliverable?**
☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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?**
☐ 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. Continuously and routinely informing the public of the high level of federal, state, and local engagement in, and commitment to election security.

6. **What metric or measurement will be used to define success?**
    a. Surveys of public concerns and confidence.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division, Statewide Voter Registration Core Team (SVRS Core Team).

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Surveys, communications activities	Secretary of State, Indiana Election Division, SVRS Core Team	75	No Response	No Response

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
No new resources required						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Increased/sustained public confidence in election outcomes. High participation in elections.

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

a. Sustained awareness efforts can improve public engagement in cybersecurity awareness and effort.

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

a. Lower public confidence in election outcomes. Public stress and anxiety. Lower participation in elections.

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

a. Responses to public surveys.

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

☐No ☒ Yes

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?

☐No ☒ Yes

a. Unknown

Other Implementation Factors

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

a. Commitment of state and local election official and administrator time and communications resources.

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

☒No ☐ Yes

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

a. Ongoing commitment of state and local election official and administrator time and communications resources.

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

a. Stakeholders within the election sector are engaged in this initiative.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors would likely benefit from ongoing public communications and outreach activities.

Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. None

Evaluation Methodology

Objective 1: The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence by November 2024.

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: Continuity, Coordination, Maintenance of Effort and Oversight

Deliverable: Continuity, Coordination, Maintenance of Effort and Oversight

General Information

1. **What is the deliverable?**
    a. Continuity, Coordination, Maintenance of Effort, and Oversight
        - To assure the highest level of ongoing election cybersecurity vigilance and effort, the Secretary of State may integrate the IECC Election Committee's day-to-day, and election-to-election responsibilities with the professionally managed Indiana Statewide Voter Registration System Core Team.

2. **What is the status of this deliverable?**
☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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)?**
☐ 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. The Statewide Voter Registration System Core Team (SVRS Core Team) will oversee and coordinate IECC Election Committee activity and deliverables.

6. **What metric or measurement will be used to define success?**
    a. Ongoing effective and efficient coordination and execution of Election Committee business and deliverables.

7. **What year will the deliverable be completed?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division and SVRS Core Team.

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Transfer Election Committee administration to SVRS Core Team	Secretary of State, Election Division and SVRS Core Team	50	12/31/2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Increased efficiency and responsiveness. The SVRS Core Team is continually active, has professional administrative and technical support resources, is bi-partisan, and typically meets on a bi-weekly basis.

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

a. Increased efficiency and responsiveness. See the SVRS Core Team response in #17.

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

a. None

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

a. Acceptance by the SVRS Core Team of responsibilities associated with administration of IECC Election Committee administration.

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

☒No ☐ Yes

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?

☒No ☐ Yes

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?

☒No ☐ Yes

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

a. Possibly the SVRS Core Team will require additional administrative and technical support resources – likely provided by the Secretary of State and Indiana Election Division, on an as-needed basis.

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

a. Secretary of State, Indiana Election Division, SVRS Core Team.

27. Can this deliverable be used by other sectors?

☒No ☐ Yes,

Communications

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

a. IECC leadership, state and local 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)?

☐No ☒ Yes

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

a. None

Evaluation Methodology

Objective 1: Indiana Statewide Voter Registration System Core Team will begin formally coordinating and overseeing the deliverables of the IECC Elections Committee Strategic Plan by Dec. 31, 2021.

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 Statewide Voter Registration System Core Team will assist with all the deliverables and objective in the IECC Elections Committee Strategic Plan and report the progress to the IECC by Dec. 31 of each year.

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

There was no supporting documentation at this time.