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