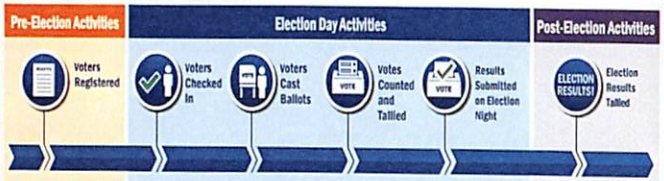
2020 Election Security Planning Snapshot
Lake County

SAFEGUARDS / RESILIENCY MEASURES

Indiana Election Process



Pre-Election Safeguards

Voters Registered

- Voter registration database is protected by firewall, security updates, and an intrusion detection/prevention system.
- Database is secured through Access Control Listing (whitelisting), logging of database changes, two-factor authentication, and threat and vulnerability testing.
- Users receive security training and follow strict security protocol.
- Database backups and contingency plans in place.

Election Day Safeguards

Voters Checked In

- Voter presents ID and is matched to voter database.
- Paper backup lists are available.
- Failsafe measures protect voter's right to vote.

Voters Cast Ballots

- Indiana's elections use optical scan ballot cards, Direct Record Electronic (DRE) / touch screen systems, and hybrid voting systems.
- Each system has specific security procedures.
- Absentee ballots tracked and kept in a secure location until the polls have closed.

Voting, Tallying, & Reporting Systems

- Specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election by non-partisan election experts.
- Voting systems are not connected to the internet.
- Ballots are securely stored with extensive chain-of-custody records.
- Electronic and physical security measures ensure voting system integrity on Election Day.
- All ballots tabulated and delivered by bipartisan teams of poll officials.

Post-Election Safeguards

Election Results Tallied

- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.
- Results are unofficial until canvass of votes.
- Vigorous chain-of-custody records maintained.

Election Day Security Guidelines

From the 2018 Indiana Election Day Handbook

Ballot and equipment security:

- Ensure that optical scan and DRE devices are properly locked and sealed.
- Ensure that ballots are issued and transported under bi-partisan supervision.

THREAT MITIGATION

Specific Threats / Mitigation

Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. ***Mitigation:*** Education and training on threats and types of targeted information; conducting phishing campaign assessment

Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. ***Mitigation:*** Clear and consistent information, including accurate cybersecurity terminology; relationship building with the media; open dialog with the public

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. ***Mitigation:*** Incident response and recovery planning; penetration testing; strong passwords and two-factor authentication, especially for admin access; encrypted password storage and transmission; active system monitoring; current security updates; upgrades to supported OS and applications; physical security measures

Distributed Denial of Service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. ***Mitigation:*** Business continuity and incident response planning; anti-virus software and firewall; good security practices for distributing email addresses; email filters

Insider Threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. ***Mitigation:*** Background checks for all election workers and contractors; insider threat training; vigorous chain-of-custody records; strict access controls based on need and updated as access needs change

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy (www.belfercenter.org/D3P)

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices *(NIST Pub. 800-61)*

If you suspect a Cybersecurity Incident has occurred, contact—

- Indiana Secretary of State Chief Information Officer, 1-866-461-8683
- Cybersecurity and Infrastructure Security Agency (CISA), (888) 282-0870 or cisacustomerservice@cisa.dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

For Additional Information or Questions

Indiana Secretary of State's Office: 1-866-IN-1-VOTE (1-866-461-8683); sos@sos.in.gov

Cybersecurity and Infrastructure Security Agency: www.dhs.gov/cisa/election-security

- Tony Enriquez, Region V Cybersecurity Advisor, antonio.enriquez@hq.dhs.gov
- Alexander Joves, Region V Director for Infrastructure Protection, ipregionSops@hq.dhs.gov

2020 ELECTION INITIATIVES

Lake County Election Data

Precincts: 525
Registered Voters: 359,479
Optical Voting System: MicroVote/Chatsworth ACP 2200
Accessible Voting System: Infinity VP-1 4.3
E-Poll Book Systems: KNOWiNK
Website: https://www.lakecountyin.org/

2020 Election Preparation Activities

1. Partner with the Indiana National Guard and Incident Response Cybersecurity Committee to establish incident response plans through table-top exercises and incident response plan testing.
2. Continue partnership with CISA to evaluate additional intrusion detection device installations at the county or state level and evaluate CISA Risk and Vulnerability Assessment findings to implement improvement opportunities.
3. Implement two-factor authentication to access statewide voter registration system and conduct cybersecurity training.
4. Evaluate election purposed computers (laptops or desktops) or virtual machines to harden election system network connections and replace unsupported operating systems or internet browsers.
5. Evaluate electronic poll book vendor controls, software and patch updates, and security protocols.
6. Evaluate election night reporting systems to identify improvement opportunities for data entry authentication, data backups, and intrusion detection.
7. Conduct third-party penetration testing of SVRS, electronic poll books, and other related election system infrastructure.
8. Implement SVRS security scans for file uploads for all users.
9. Implement email encryption and digital signatures for file transfers and transmission of election data.