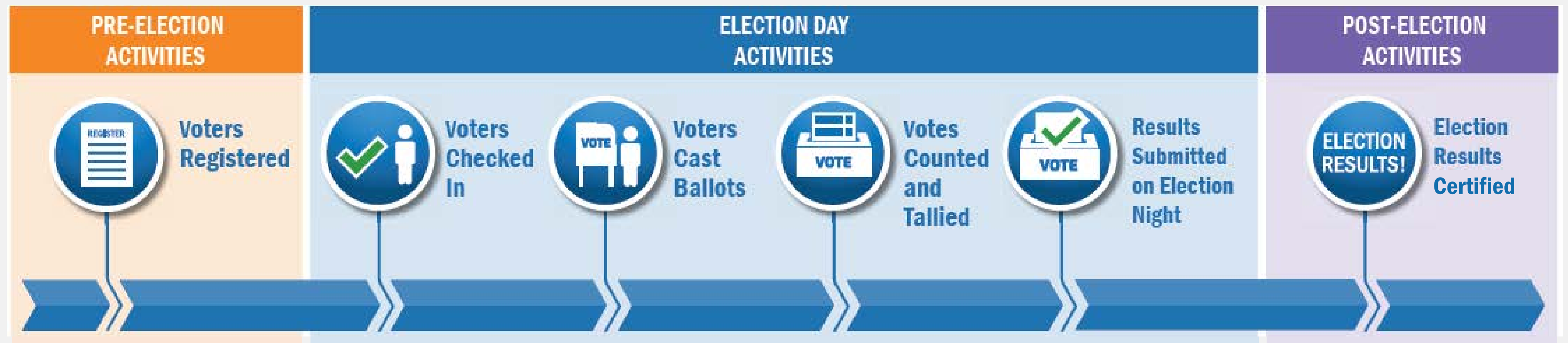
2018 Election Cybersecurity Planning Snapshot

Polk County

ACTIVITIES / SAFEGUARDS

Iowa Election Process



PRE-ELECTION SAFEGUARDS

Voters Registered

- Voter registration database is protected by firewall and security updates.
- Database is secured through Access Control Listing (whitelisting) and two-factor authentication.
- Users receive security training and follow strict security protocol.
- Database backups and contingency plans in place.

ELECTION DAY RISK 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

- Iowa's elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Absentee ballots are tracked and kept in secure location.

Voting, Tallying, & Reporting Systems

- County-specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election – open to the public.
- Voting systems are not connected to the internet.
- Ballots are securely stored with extensive chain-of-custody records.
- Electronic and physical security measures insure voting system integrity on Election Day.

POST-ELECTION RISK SAFEGUARDS

Election Results Canvassed

- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.
- Vigorous chain-of-custody records maintained.
- Post-election audit performed on random selection of all precincts.

Election Day Security Guidelines

From Office of the Secretary of State Pursuant to Iowa Code 49.126

Ballot security: Precinct officials must safeguard ballots at all times. It is illegal to take a ballot from the polling place, curbside voting is the only exception. PEOs shall report any person removing a ballot from polling place to the county auditor immediately.

Equipment security: Precinct officials must safeguard voting equipment and all accessories at all times. Do not allow unauthorized persons access to this equipment. Only persons with written authorization from the county auditor may attempt to repair or replace malfunctioning machines. Call the County Auditor's Office immediately if any of the security seals are broken.

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*: Cyber hygiene training (see initiatives) which includes Securing the Human training

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 and 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 planning, penetration testing, two factor authentication, recovery planning active system monitoring and current security updates along with 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 your email address, 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—

- ✓ Iowa Office of the Chief Information Officer - Information Security Division, (515) 281-5503 or https://iso.iowa.gov/contact-information-security-office
- ✓ National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.dhs.gov
- ✓ Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

In the event of a Data Breach, notify—

- ✓ Iowa Office of the Attorney General - Consumer Protection Division, consumer@iowa.gov or (515) 281-5926. More information at https://www.iowaattorneygeneral.gov/ for-consumers/security-breach-notifications

For Additional Information or Questions

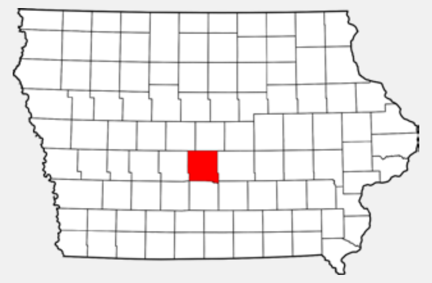
Iowa Secretary of State's Office: Ken Kline, Deputy Commissioner of Elections, ken.kline@sos.iowa.gov

U.S. Department of Homeland Security: www.dhs.gov/topic/election-security

- ✓ Geoffrey Jenista, Region VII Cybersecurity Advisor, geoffrey.jenista@hq.dhs.gov
- ✓ Phil Kirk, Region VII Director for Infrastructure Protection, ipregion7@hq.dhs.gov

2018 ELECTION INITIATIVES

Polk County Overview



Precincts – 177

Active Voters – 281,315 (as of June 2018)

Optical Voting System / Model – Unisyn OVO v. 1.33M

Accessible System / Model – Unisyn OVI VC

Website – www.polkcountyiowa.gov/auditor/election

2018 Activities & Timeline Checklist

☑ Initiative 1: Cybersecurity workshop with auditors and IT staff from across the State
(Target Completion: June 22)

☐ Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at https://learn.cisecurity.org/ei-isac-registration
(Target Completion: July 15)

☐ Initiative 3: Develop County Incident Response Plan including Reporting Matrix
(Target Completion: August 1)

☐ Initiative 4: Schedule Cyber Hygiene Scanning. Contact nccicustomerservice@hq.dhs.gov and reference "Iowa Cyber Hygiene Initiative" to obtain this service free through DHS
(Target Completion: September 1)

☐ Initiative 5: Complete "Securing the Human Training." Contact IVoters.support@sos.iowa.gov to schedule
(Target Completion: September 1)

☐ Initiative 6: Register for services provided by the Iowa Office of the Chief Information Officer
(Target Completion: September 1)

DEVELOPED BY THE IOWA SECRETARY OF STATE

W/ SUPPORT FROM THE US DEPARTMENT OF HOMELAND SECURITY – ELECTION TASK FORCE