Homeland Security

MAY 2018

Election Infrastructure Cyber Risk Scenarios

PREELECTION ACTIVITIES

Voters Registered

ELECTION DAY ACTIVITIES

Voters Checked In

Voters Cast Ballots

Votes Counted and Tallied

Results Submitted on Election Night

POSTELECTION ACTIVITIES

Election Results Tallied

PREELECTION RISK SCENARIOS

- Voter information in a voter registration system is manipulated.
- A voter registration system is disrupted.
- Voter information in a voter registration system is exposed.

ELECTION DAY RISK SCENARIOS

Votes cast in a voting machine are manipulated covertly.

- Votes cast in a voting machine are manipulated overtly.
- Voting machines and related information technology (IT) are disrupted.
- Infrastructure necessary to transmit absentee ballots is disrupted.
- Vote selections on a ballot are exposed.

POSTELECTION RISK SCENARIOS

- Results in official vote tabulation systems are manipulated.
- Unofficial results for reporting on Election Night are manipulated.
- Unofficial results reporting on Election Night is disrupted.

Anecdotes of Election Security Engagement

CALIFORNIA

State of California

- California has one of the most strenuous voting system testing and certification programs in the country, which requires months of testing on functional testing, source code review, red team security testing, as well as accessibility and volume testing.

- Conducted an agency-wide security audit:
  - Identified high risk systems, decommissioned said systems, and replaced them;
  - Upgraded firewalls;
  - Increased 24/7 monitoring and alert capabilities;
  - Strengthened agency policies to harden procedures related to security;
  - Implemented cybersecurity tools to detect and prevent malware and viruses; enhanced the security of servers;
  - Hosted cybersecurity training for county officials;
  - Added redundancies to systems to mitigate the impact of potential outages;
  - Increased collaboration between federal, state, and local partners.

Orange County, CA:

- Developed an extremely robust county cybersecurity plan. The plan was coordinated with and reviewed by DHS. Included in the plan were items such as:
  - Encrypted communications including email
  - 2 factor authentication
  - Phishing training and testing for all election department employees.
  - Comprehensive incident response plan
  - Additional network monitoring and intrusion detection
  - Risk limiting audits to be put in place

Los Angeles County, CA:

- Has undertaken a multi-year effort to design their own voting system. The voting system is designed to support risk-limiting audits, provide redundancy throughout the counting process through a back-end tabulation structure that can recreate the election ballot by ballot and offer full transparency. This is a first of its kind effort where the county will own its own software.

COLORADO

State of Colorado

- First state in the nation to conduct a statewide risk limiting audit.
- State conducts state-level asset assessment of the counties and runs remote scans of county systems.
- State requires counties to take regular cybersecurity training and does phishing assessments of the counties.
- State implemented updates to statewide database including requiring two-factor authentication for access to statewide voter registration database.

City of Denver, CO

- Implemented a county-wide cyber monitoring task force to support the election office. Because the city of Denver is in charge of the airport networks, they already had advanced monitoring and response capabilities. Now the election division is tied into this information sharing.
- On Election Day the county sets up a command center with election employees and county IT employees monitoring network activity, social media, and other indicators to be able to detect and respond to possible incidents. The state of CO has access to this info via Denver and shares it with counties across the state.
- 2016 marked the first time the City and County of Denver and the Colorado Secretary of State worked together to share network traffic information, jointly utilizing tools provided by the Colorado Division of Homeland Security. This strong intergovernmental collaboration, alongside the pre-election validation of equipment and day-of monitoring, ensured that election integrity remained intact.

FLORIDA

State of Florida:

- Governor has funded Secretary of State to establish cyber navigators to support county election officials in conducting risk assessments, putting mitigations in place and providing Election Day support.
- State is deploying intrusion detection ALBERT sensors to all county election offices.
- State is requiring statewide cyber training prior to November election.

Escambia County, FL

- Working with the University of West Florida Center for Cybersecurity to conduct trainings and table top exercises.
- Using CloudFlare website support to protect from DDOS and SQL injection attacks.
- Have deployed intrusion detection ALBERT sensor already.
- Hired an elections infrastructure security officers to lead this charge.

INDIANA

State of Indiana:

- Using DHS services (have discussed this in general publicly), are EI-ISAC members, have deployed an intrusion detection ALBERT sensor on state network, and appreciate DHS' information sharing.
- Conducted a self-evaluation against the CIS recommendations. This led to, among other things, an upgrade to their statewide database to include two-factor authentication with USB keys, increased access controls, and monitoring including after-hours restrictions and monitoring.

PENNSYLVANIA

State of Pennsylvania

- Recently announced that all counties must move off paperless DRE's prior to 2020 election.
- State is fully engaged with DHS and taking advantage of a number of services including RVA, CyHy, and Hunt. ALBERT sensor is deployed.
- State is in process of upgrading Statewide Voter Registration Database (SWVRD) and other networks to improve intrusion detection and include two-factor authentication.

WASHINGTON

State of Washington:

- Building an Office of Secretary of State security operations center (SOC) compliant with federal and state recommendations.
- Upgraded all firewalls and network protections. Installed additional network monitoring.
- Created a state-level cyber unit whose mission is to support county level risk planning and incident response.

Homeland Security

May 2018

Election Infrastructure - Cybersecurity

PRE-ELECTION ACTIVITIES

Voters Registered

ELECTION DAY ACTIVITIES

Voters Checked In

Voters Cast Ballots

Votes Counted and Tallied

Results Submitted on Election Night

POST-ELECTION ACTIVITIES

Election Results Tallied

CYBERSECURITY CONSIDERATIONS

Auditability

To enhance election system integrity, states are prioritizing the purchase and deployment of auditable voting systems. Post-election audits are an important step to ensuring the integrity and resilience of the process. Consider using funding to hire temporary staff for organizing and running post-election audits. This can quickly improve the efficiency and effectiveness of the audit process and lessen the burden on overworked and understaffed election offices.

Planning and Exercises

A comprehensive, well-practiced incident response plan can ensure a resilient process, enabling response and recovery from potential disruptions. Election officials are natural contingency planners and many already have well-thought-out contingency plans. Consider using resources and funding to update existing plans, to include the development, implementation, and training of cyber-incident response. Developing and exercising these plans can be a relatively low-cost, high-benefit area of focus.

Training

All election staff have a responsibility to keep our elections systems secure. Regular training and testing raises awareness on cybersecurity best practices. Consider funding and implementing cybersecurity training for all staff, not just IT professionals.

Defensibility

Defensibility begins with an understanding of which systems and data need to be defended. Understanding the high-value/high-risk components of election IT systems allows for prioritization of funding. Consider investing in full system architecture reviews, which can be a critical starting point for risk mitigation decisions.

Resilience

The ability to detect, defend, mitigate, and recover from cyber incidents is critical to maintaining the integrity of the election process. Consider investing in regular online and offline backups of critical data (e.g., voter registration data). Testing and refining backup methods can improve the election system's ability to recover from ransomware or other cyber attacks intended to destroy or alter data.

Homeland Security

May 2018

Immediate Resources for Election Officials

The most valuable resource election officials have is time. Every day they are one day closer to another election which means they literally have no time to waste. Identifying the risks to their systems and possible solutions can be time consuming and costly for local election officials who have neither time or money to waste. But a solution exists: The Department of Homeland Security's National Protection and Programs Directorate (NPPD) offers cyber expertise and services at no cost to election officials to augment their arsenal of cybersecurity tools.

NPPD offers a broad range of cyber products and services free to state and local election officials including network and system assessments either self-administered or undertaken by NPPD staff; alerts and bulletins; best practices; and mitigation and incident response.

Local election officials can immediately begin to improve their cybersecurity position through three simple, straightforward steps:

Step 1: Know Your System

Knowing your elections infrastructure means knowing your network and system vulnerabilities and warning signs of strange network behavior – known as "anomalies" – and knowing what to do about them.

DHS offers Vulnerability scanning of Internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation's overall resiliency.

Administered by NPPD staff experts, the assessment takes place during a one-week period. After the assessment's conclusion, elections officials will receive an in-depth report of key discoveries and practical recommendations for improving an organization's cybersecurity operation to mitigate known vulnerabilities and sure up its defenses. After the initial report participating election offices will receive ongoing reports every week for continued improvement and response to evolving threats to election systems. **For more information and to arrange the assessment, contact** ncciccustomerservice@hq.dhs.gov.

Step 2: Know Your Staff Needs To Withstand Phishing

Elections are at their core a human activity. Election officials rely on professional and temporary staff to support any election. Awareness and training of that staff is critical to improving the security of the election process. Strengthen your elections infrastructure through NPPD's **Phishing Campaign Assessment**, which measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks.

Administered by NPPD staff, the assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and the more personalized spear-phishing attacks. **For more information and to arrange the assessment, contact** ncciccustomerservice@hq.dhs.gov.

Step 3: Join the EI-ISAC

Begin improving your cybersecurity status with information sharing. You can't secure your election infrastructure without knowing the threats to protect against, assets to protect, and how to protect them.

Join (for free!) the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). This information sharing center was created to serve the election community by providing near real time threat and risk sharing as well as cybersecurity best practices geared towards election officials.

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on election infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors. The EI-ISAC supports the election infrastructure community through:

- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices
- 24 x 7 x 365 network monitoring (paid-service option)

Membership in the EI-ISAC is open to all state, local, tribal, and territorial (SLTT) government organizations and associations that support elections in the United States. DHS encourages state and local elections agencies to use this initiative to receive the information they need to help protect their systems. **To join the EI-ISAC, please complete the registration form** https://learn.cisecurity.org/ei-isac-registration.

Election Anecdotes

CALIFORNIA

Los Angeles County, CA

- Multi-year effort to design their own voting system. The voting system is designed to support risk-limiting audits, provide redundancy throughout the counting process through a back-end tabulation structure that can recreate the election ballot by ballot and offer full transparency. This is a first of its kind effort where the county will own its own software.

Orange County, CA

- Developed a county cyber security plan. Included in the plan were items such as:
    - Encrypted communications including email
    - 2 factor authentication
    - Phishing training and testing for all election department employees
    - Comprehensive incident response plan
    - Additional network monitoring and intrusion detection
    - Risk limiting audits to be put in place

California SOS and Masterson Testimony:

- Hearing Recording: California SOS and Masterson testimony and many resources regarding CA's cyber/elections initiatives: http://selc.senate.ca.gov/content/oversightinformational-hearings
- Overview of California election law prior to 2016 Presidential Election:
    - State law requires that no voting system or part of a voting system can be connected to the internet.
    - California has one of the most strenuous voting system testing and certification programs in the county, which requires months of testing on functional testing, source code review, red team security testing, as well as accessibility and volume testing.
    - California counties are required to perform logic and accuracy testing of their voting systems before each election and follow specific procedures for programing, deployment, and the use of voting equipment.
    - Californians, for the most part, cast their votes on paper ballots. Of the limited voting systems that include a direct record electronic system, they must have Voter Verified Paper Audit Trail (VVPAT)
    - VoteCal (statewide voter regional database system) standards meet the standards of NIST, DHS, and NASS. Resides on servers located on a secure internal network. Vote Cal's data does not reside in the cloud, and there is no access between the public website servers and the database servers, which is where the voter registration data resides. State routinely scans and applies patches to VoteCal.
- Since 2018, California has done the following:
    - Conducted an agency wide security audit, identified high risk systems, decommissioned said systems, and replaced them; upgraded firewalls; increased 24/7 monitoring and alert capabilities; strengthened agency policies to harden

procedures and processes related to security; implemented cybersecurity tools to detect and prevent malware and viruses; enhanced the security of servers; hosted cybersecurity training for county officials; added redundancies to systems to mitigate the impact of potential outages; and increased collaboration between federal, state, and local partners.

- Ongoing need for additional resources:
    - Increased in technology staff at state and county level
    - Increased funding for county election officials, especially concerning voting systems that are meeting their life expectancy. "County voting machine are literally falling apart" – SoS Padilla

COLORADO

State of Colorado

- First state in the nation to conduct a statewide risk limiting audit.
- State conducts state level asset assessment of the counties and runs remote scans of county systems.
- State requires counties to take regular cyber security training and does phishing assessments of the counties.
- State implemented updates to statewide database including requiring two factor authentication for access to statewide voter registration database.
- https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/10/the-cybersecurity-202-how-colorado-became-the-safest-state-to-cast-a-vote/5af317c930fb042db5797427/?utm_term=.269ba96f6a84

City of Denver, CO

- Have implemented a county-wide cyber monitoring task force to support the election office. Because the city of Denver is in charge of the airports networks they already had advanced monitoring and response capabilities. Now the election division is tied into this information sharing.
- On Election Day the county sets up a command center with election employees and county IT employees present monitoring network activity, social media and other indicators to be able to detect and respond to possible incidents. The state of CO has access to this info via Denver and shares it with counties across the state.
- 2016 marked the first time the City and County of Denver and the Colorado Secretary of State worked together to share network traffic information, jointly utilizing tools provided by the Colorado Division of Homeland Security. This strong intergovernmental collaboration, alongside the pre-election validation of equipment and day-of monitoring, ensured that election integrity remained intact.
- https://www.denvergov.org/content/denvergov/en/technology-services/news/2017/denver-takes-home-cybersecurity-award-for-2016-elections-.html

FLORIDA

State of Florida:

- Governor has appropriated money to Department of State to establish cyber navigators to support county election officials in conducting risk assessments, putting mitigations in place and providing election day support.
- (b)(7)(E)
- State is requiring statewide cyber training prior to November election.
- EAC and DHS are conducting a training there in May. EAC has already done two trainings with local supervisors of elections.
- http://www.northescambia.com/2018/05/florida-to-beef-up-elections-cybersecurity

Escambia County, FL

- Working with the University of West Florida Center for Cybersecurity to conduct trainings and table top exercises.
- (b)(7)(E)
- http://wuwf.org/post/uwf-center-cybersecurity-fdle-hold-cyber-preparedness-courses

IDAHO

State of Idaho

- News article about election software upgrades: http://www.spokesman.com/stories/2018/feb/04/idaho-secretary-of-state-seeks-budget-boost-to-upg/

ILLIONIS

State of Illinois

- At the June 20-21 Illinois Elections Cybersecurity Conference in Bloomington-Normal, IL, DHS/CIS/EAC will put on following:
  - June 20 Day 1 - Belfer Center TTX fully supported by DHS, EAC, CIS.
  - June 21 Day 2 - 6-hr Training EAC-led with DHS Matt Masterson Support.

Cook County, IL:

- Built an election protection framework called Defend, Detect, Recover. Align almost entirely with NIST cyber framework.
- As part of that exercise have systematically mapped every system, ID'd every known vulnerability point, and built/defined defenses, detection methods, and recovery plans.
- Now in the process of testing/practices all of recovery (incidence response) plans. This is both in cyber realm and physical procedural realm. Trying to ensure all of paper based mitigations are well defined and that those responsible for implementing them can understand our instructions.
- Additionally, have benchmarked ourselves against the best election protection and cyber protection documents out. They all rely on very similar controls in the cyber realm. CIS, Belfer, etc. Working through the process of instituting the controls currently not in full use; or accepting risks.
- Hired an elections infrastructure security officers to lead this charge.

- At State Level Cook Co has led a task force of Feds, FBI, DHS, and State Elections, State CISO, State Police, and then local election officials. We are driving to have state board lead - through they are very remiss to do so.

INDIANA

State of Indiana:

- They are using our scanning services, are EI-ISAC members, and appreciate the information sharing we provide.
- Have conducted a self-evaluation against the CIS recommendations. This led to, among other things, an upgrade to their statewide database to include 2 factor authentication with USB keys, increased access controls and monitoring including afterhours restrictions and monitoring.

IOWA

State of Iowa

- Recently created a statewide cyber security task force to communicate risks, provide mitigation strategies and prepare incident response plans. DHS is part of this task force.
- Have conducted statewide training with local election auditors to ensure awareness to the threats as well as state specific mitigations.
- Have implemented improvements to the statewide networks including two-factor authentication and limiting access at non-work hours unless approved by a network administrator.
- State IT and County IT are working in collaboration to provide free training and exercises including phishing assessments.

KENTUCKY

Kentucky Election Clerks Receive Cybersecurity Training:

- On 19 April 2018, in conjunction with the Kentucky County Clerks Association meeting, DHS presented cybersecurity training to clerks from all 120 counties in Kentucky. Secretary of State Alison Lundergan Grimes, reported to media sources: "Kentucky is the first state in the nation to conduct the training." The training was in preparation in advance of the May 22 primary election in Kentucky.
- Secretary Grimes announced DHS officials and other partners will conduct statewide cybersecurity briefings and trainings for Kentucky's 15,000 precinct election officials and media this summer. Kentucky has 3,700 precincts and 15,000 precinct officer/workers.
- Kentucky has contracted with a cyber security firm to audit the election process and develop protections against hostile interference."
- The Kentucky State Board of Elections has also moved to require future election equipment provide a voter-verified paper trail. Federal funding will help Kentucky transition to a fully paper-backed voting system.
- "The Department of Homeland Security values our partnership with Secretary of State Grimes as we work together with Kentucky and other states to improve the security of the election process," said Matt Masterson, senior cybersecurity advisor at DHS. "We

appreciate the commitment and dedication that election officials across the state have demonstrated to ensuring secure and resilient elections for Kentucky voters. We look forward to our continued partnership with Secretary Grimes and state and local officials across the nation as we work to maintain the integrity of America's election infrastructure system."

MINNESOTA

State of Minnesota

- On Wednesday, May 16, 2018, SoS Simon and other election officials urged the state legislature to free up federal funds for election security by passing an authorizing bill. The authorizing bill must be passed soon, as the legislature finishes their session this weekend. (AP Report)

NEVADA

State of Nevada:

- All counties in the state will have new voting systems and epollbooks prior to June 12 thanks to $8 Million dollar funding allocation from state legislature.
- Local election officials will be required to receive cyber training in near future.
- Upgrading statewide voter registration database with additional protection and detection measures.
- https://www-reviewjournal-com.cdn.ampproject.org/v/s/www.reviewjournal.com/news/politics-and-government/nevada-takes-measures-to-ensure-election-security/amp/?amp_js_v=0.1&usqp=mq331AQGCAEYASgB#origin=https%3A%2F%2Fwww.google.com&prerenderSize=1&visibilityState=prerender&paddingTop=54&p2r=0&horizontalScrolling=0&csi=1&aoh=15260673529198&viewerUrl=https%3A%2F%2Fwww.google.com%2Famp%2Fs%2Fwww.reviewjournal.com%2Fnews%2Fpolitics-and-government%2Fnevada-takes-measures-to-ensure-election-security%2Famp%2F&history=1&storage=1&cid=1&cap=swipe%2CnavigateTo%2Ccid%2Cfragment%2CreplaceUrl

NEW JERSEY

State of New Jersey

- (b)(7)(E)
- NJOHSP is offering the counties free online cybersecurity training.
- In early September of 2016 the State had its Statewide Voter Registration System vendor (Everyone Counts) have Rapid 7 conduct a vulnerability assessment including penetration testing.
- The State has mandatory Seal-Use Protocols to help secure the voting machines. (Attached)
- The State has mandatory Pre-Election Testing Protocols for testing the voting machine for accuracy.

- https://www.njhomelandsecurity.gov/media/joint-release-concerning-the-cybersecurity-of-new-jerseys-election-systems?rq=election%20training
- The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is the State's one-stop shop for cybersecurity information sharing, threat analysis, and incident reporting. Learn more about the NJCCIC's mission https://www.cyber.nj.gov/.
- The New Jersey Office of Homeland Security and Preparedness (NJOHSP) leads and coordinates New Jersey's counterterrorism, cybersecurity, and emergency preparedness efforts while building resiliency throughout the State. https://www.njhomelandsecurity.gov/.

NORTH CAROLINA

State of North Carolina –

- Openly talks about taking advantage of our services including RVA and CyHY. They have bragged about our "deepening relationship" (http://www.charlotteobserver.com/opinion/op-ed/article202454724.html). In addition, they are using free DDOS protection from one of the vendors providing it to election officials. In addition NC has good post- election auditing procedures.

OHIO

State of Ohio

- Secretary Husted is taking advantage of a wide array of our services to ensure they have taken every step possible. In addition, Ohio is actively pushing counties to take advantage of our services by signing up for EI-ISAC, CyHY and phishing evaluations (https://www.sos.state.oh.us/globalassets/elections/directives/2017/dir2017-19.pdf).
- Ohio has engaged the National Guard to do evaluations. SOS Husted has also pushed to improve post-election auditing procedures including encouraging counties to conduct RLA's.
- https://www.washingtontimes.com/news/2016/nov/1/national-guard-cybersecurity-team-helps-secure-ohi/

Franklin County, OH

- On May 17, 2018, the Franklin County Board of Elections announced the installation of a (b)(7)(F) designed to provide even greater cyber security protection to Franklin County's cybersecurity defense system.
- The new relationship with EI-ISAC also offers Franklin county other cybersecurity related resources such as Incident Response and Remediation; Threat and Vulnerability Monitoring; a Best Practices Clearinghouse; and Election Specific Threat Intelligence.

PENNSYLVANIA

State of Pennsylvania

- Recently announced that all counties must move off paperless DRE's prior to 2020 election.

- State is fully engaged with DHS taking advantage of a number of services including RVA, CyHY and Hunt. Albert sensor is deployed.
- State is in process of upgrading Statewide Voter Registration Database (SWVRD) and other networks to improve intrusion detection and include two-factor authentication.

RHODE ISLAND

State of Rhode Island

- Created a state level election task force involving the SOS, GOV, DHS and others.
- Conducting a state and local level TTX to exercise response plans, improve awareness among local election officials and push for additional mitigations to known risks.
- After deploying new voting system statewide in 2016 they will be piloting and moving toward risk limiting audits statewide. This would make them the second state and first one that is precinct based (CO being centrally counted) to run RLA's.
- Moving forward with 2FA for SWVRD.

VIRGINIA

Fairfax County, VA

- Our elections task force just visited with them and came away impressed with their preparation and how seriously they were taking the security of the process. Heard a perfect example of how our information sharing is working. Fairfax received our Cisco router alert via EI-ISAC, took their routers offline, and evaluated the risks, upgraded where necessary and redeployed with mitigations in place.

WASHINGTON

State of Washington:

- Building an Office of Secretary of State SOC compliant with federal and state recommendations for SOC.
- Have upgraded all firewalls and network protections. Installed additional monitoring of networks.
- Created a state level cyber unit whose mission will be to support county level risk planning and incident response (similar to what they did to develop the best state and local continuity of operations plan I have seen).
- After giving counties support and allowing for improvements they will be auditing counties against known controls like CIS and Belfer.
- Engaged with National Guard to provide cyber evaluations and support to state and local level officials.
- https://www.king5.com/article/news/politics/national-guard-to-tighten-election-security-in-washington/281-547445329

WEST VIRGINIA

State of WV

- Have hired a National Guard member on staff to sit in Fusion center and monitor activity directed at statewide systems. National Guard member reports directly to CIO and SOS and provides bi-weekly reports regarding activity.
- Had four National Guard members on duty on election day to provide monitoring and rapid deployment in the case of a cyber incident.
- Highly engaged with the Belfer center project using the info to evaluate and upgrade state systems as well as train and improve local election officials.

WISCONSIN

State of Wisconsin

- The Wisconsin Elections Commission is moving ahead with using electronic poll books, instead of the paper ones used now, to check in voters at polling places. Five electronic poll books, dubbed Badger Books, will be in place at five polling stations in the April 3 spring election as part of a pilot program. They will be used in Brookfield, Mequon, Sun Prairie, Beloit and the Town of Trenton in Washington County. The electronic poll books, that can also be used to register voters, process an absentee ballot and other election-related activities, are scheduled to be used statewide in the Aug. 14 primary and Nov. 6 midterms.
- https://www.usnews.com/news/best-states/wisconsin/articles/2018-03-13/wisconsin-election-security-focus-of-testing-planning
- On April 18, 2018 "The Wisconsin Elections Commission unanimously approved moving forward with tapping a $7 million federal grant to hire additional staff and enhance security protections ahead of the fall elections. The commission voted to proceed with hiring up to six new staffers, although exactly how many and in what positions will be determined later. It also backed going ahead with purchasing multi-factor authentication software to improve security in Wisconsin's voter registration database accessed by clerks and other election officials, and contracting with information technology specialists to address immediate security needs. The two IT contracts would be no more than $225,000 each while creating the multi-factor authentication process — where users of the voter database would have to enter a password and then a second factor, like a randomly generated number sent by email — is to cost no more than $200,000. Such a system is seen as a strong deterrent to hackers. Additional spending may target the needs of nearly 2,000 municipal election clerks. Before any of the money can be spent, Gov. Scott Walker's administration must give approval to release the grant funds to the commission."
- https://www.usnews.com/news/best-states/wisconsin/articles/2018-04-18/wisconsin-elections-commission-approves-spending-on-security