Checklist for Securing Election Night Results Reporting

Election Night Reporting (ENR) systems consist of aggregating and displaying unofficial election results to the public, usually through an official website or social media platforms. The election results reported on election night are never the final, certified results. However, the public often perceives unofficial election results, even on election night, as final.

There are several reasons vote totals change, including adding eligible late-arriving mailed ballots and provisional ballots to the final tally. The timeframe for local election officials to complete the certification process ranges from one to 30 days after the election. It is important for election officials to provide context when sharing election results after polls close on election night until results are certified.

Election officials need to provide assurance to the public that the ENR system data is accurate and protected. Moreover, in case of a failure of the ENR system, election officials must develop backup plans and alternative methods of communicating election results. See, Best Practices: Election Results Reporting for more information about sharing election results: https://www.eac.gov/election-officials/election-results-reporting

Election officials can use this checklist as a baseline to assess their current ENR cybersecurity protocols. These protocols would be in addition to other physical and administrative procedures election officials implement to ensure data reliability, including documented chain of custody, data verification procedures, and using certified technology to tabulate vote totals.

Cybersecurity Checklist

- ◯ **Antivirus Software** – Update and run antivirus and malware detection software along with all other updates and patches.
- ◯ **Authentication** – Enable multi-factor authentication for the uploading of results and remote administration of the ENR. Enforce the use of strong passwords and proper password management. Every account should have its own password and passwords should not be written down or placed in public view.
- ◯ **Backups** – Run back-ups of election results reports on a regular schedule, such as after every update provided to the public, so that data can be recovered quickly and restored in the event of an incident. A printed copy (electronic or hardcopy) of the results can be provided if the ENR system is not operable. The backup and restore process should be tested and validated. Timestamped hardcopies should be printed at regular intervals throughout election night.
- ◯ **Backup Site –** Determine if a backup site could be available, using less bandwidth with simpler content. In the event of the main site being unavailable, it should be possible to switch to the backup, by redirecting the URL.

- ◯ **Data and Communications Security** – Use encryption and data integrity to protect communications over any network and while at rest. In particular, Transport Layer Security (TLS) protects traffic between the client (e.g., web browser) and the server. Then, ensure data is encrypted at rest when not in transit.
- ◯ **Detection** – Use an intrusion detection system to monitor networks for incoming and outgoing traffic, looking for signs of irregularities, such as above-average traffic (DDoS attack), large amounts of data being transmitted, etc.
- ◯ **Firewalls** – Use network firewalls to only allow incoming and outgoing traffic that is necessary for the operation of the ENR system. Unauthorized access (or attempts to access) to the data should be detected, prevented, reported, and escalated.
- ◯ **Media Handling** – Use clean, dedicated, single-use, or write-once media (e.g., USB flash drive, CD/DVD) to transfer data from the voting system to the ENR system. After transferring the data from the single-use or write-once media to the ENR system, catalog the media. This provides an archive of the results uploaded to the ENR system.
- ◯ **Monitor –** Monitor the ENR for unusual website traffic and conduct searches for false websites or social media accounts.
- ◯ **Proof** – Verify the data being posted to the ENR system match the official results from the voting system. Proofing should include two people, at a minimum, who validate that the results shown on the website match the results printed and exported from the voting system.
- ◯ **Test** – Thoroughly test the ENR system. Include results reporting via the ENR system in the Logic & Accuracy testing to validate that the data is being transferred accurately.
- ◯ **Verify Social Media accounts –** Attain verified status on social media platforms to increase trust that social media accounts are official.
- ◯ **Volume and Stress Test** – Volume and stress test the ENR system and the network to make sure that it has sufficient bandwidth to satisfy (or exceed) demand. A lack of bandwidth may allow for a denial-of-service attack to take an ENR system down. Discuss bandwidth requirements with the ENR website provider. Consider using a web analytics service to determine bandwidth requirements.
- ◯ **Vulnerability Scanning and Analysis** – Use software to identify security vulnerabilities on systems deployed in a network. Regular vulnerability scans of the ENR and other systems on the same network can often find points of weakness.
- ◯ **Update/Patch Software** – Most attacks target outdated software. Ensuring that all systems are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

Contingency Planning

Contingency planning is essential for a successful election. Having a Continuity of Operations Plan (COOP) allows election officials to build resiliency and more quickly recover from emergencies. Election officials should develop a detailed plan for communicating election night results, detailing how election results will be shared throughout the election, including a timeline of election results updates and which ballots are expected to be included in each report (I.e., early voting, by-mail, and absentee, Election Day provisional, write-in votes, etc...). The plan should include information about how the public can access results if results reporting websites or social media platforms are not operating as expected, or if they are rendered inoperable due to a power outage, cyber-incident incident, or any other technical failure. Contingency plans should identify threats and establish an action plan. Contingency plans can be tested using tabletop or similar exercises.

Developing a COOP

- ◯ **Maintain an up-to-date inventory of networks and diagrams** for all networks that host computers used to upload and manage election night results, including:
  - Name
  - Functionality
  - Hostnames and Ip Addresses
  - Vendor information
  - Ports used
  - Physical location
  - Any other information that would be important to respond to a network-related cybersecurity incident
- ◯ **Compile a detailed list of resources** and election night contact information (including personal phone numbers and emails) needed to troubleshoot election night results reporting issues, including:
  - Election night contact information for vendors (if the ENR is vendor supported)
  - Election night contact information for local IT support staff
  - Election night contact information for the statewide elections office, if required to report to the state in that election
  - Results reporting website URLs
  - Social media account handles
- ◯ **Develop an Incident Response Plan** that details how to respond to incidents that compromise the availability or integrity of the ENR system. The response plan should include:
  - Detailed chain of custody procedures for all election materials used to aggregate and report election results
  - Organizational charts to help employees understand how their role fits within the larger organization
  - Layouts and forms typically used for election results reporting, including detailed instructions on how to access and update election results information
  - Procedures for what steps will be taken for each type of incident (I.e. DDoS attack, power outage, etc...), and who is responsible for each step in the process during an incident
  - Plans for both physical and cyber security threats, including policies on restricted access, visitors, training, and password requirements
- ◯ **Develop an emergency communication plan** for delays in election night results reporting. Publicize how election results will be shared, and who to contact if websites or social media platforms are not operating as expected. Communication plans should include:
  - Who needs to be contacted to be informed of delays in election results reporting (e.g., County/City Administrator, IT staff, media, candidates, etc.) and their contact information
  - Who is responsible for contacting vendor and/or IT support staff
  - Who is responsible for activating back-up election results sites and redirecting URLs, as per the jurisdiction's Incident Response Plan
  - How the public can obtain election results if websites and/or social media are not operating as expected (e.g., hotline, email, printed results available for candidates and media at election office)
  - Who is responsible for communicating delays to the public
  - How to recover social media accounts

Additional Resources

Additional technical resources from the EAC and partner organizations can be found here:

- **U.S. Election Assistance Commission (EAC)**
  - Cybersecurity Risk Management for Election Officials Webinar (registration required)
  - Election Security Risk Profile Tool
  - Election Results, Canvass, and Certification
- **Center for Internet Security (CIS)**
  - Center for Internet Security (CIS), Best Practices for Non-Voting Election Technology
  - The Elections and Infrastructure Sharing and Analysis Center (EI-ISAC)
- **Cybersecurity and Infrastructure Security Agency (CISA)**
  - Department of Homeland Security (DHS) Best Practices for Continuity of Operations (Handling Destructive Malware)
  - CISA Election Results Reporting Risk Mitigation
  - CISA Cyber Resource Hub: Cyber Resource Hub | CISA
  - Cyber Incident Detection and Notification Planning Guide for Election Security Election Infrastructure Security | CISA
- **National Institute of Standards and Technology (NIST)**
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52r2, Guidelines for the Selection, Configuration, and Use of TLS Implementations
  - NIST SP 800-63-3, Digital Identity Guideline
  - NIST SP 800-94r1 – Guide to Intrusion Detection and Prevention Systems (IDOS)
  - NIST SP 800-184 Guide for Cybersecurity Event Recovery
  - NIST SP 800-41r1, Guidelines on Firewalls and Firewall Policy
  - NIST SP 800-61r2, Computer Security Incident Handling Guide
- **U.S. Department of Justice (DOJ)**
  - Ransomware: What It Is and What To Do About It