U.S. ELECTION ASSISTANCE COMMISSION (/)

DOCUMENTS

CHECKLIST

CHECKLIST FOR SECURING ELECTION NIGHT REPORTING SYSTEMS (/DOCUMENTS/2017/10/23/CHECKLIST-FOR-SECURING-ELECTION-NIGHT-REPORTING-SYSTEMS-DATA-ELECTION-ADMINISTRATION-SECURITY)

Posted:Oct 23 , 2017

The EAC has led the way in ensuring voting systems brought to the market are vigorously tested against Voluntary Voting System Guidelines (VVSG), including security requirements and the capability to accurately report election results.

Many jurisdictions also use a separate Election Night Reporting (ENR) system to display ***unofficial*** election night results to the public through a web-based application. Results do not become official until certified by the state after an official post election canvassing process.

▢ **Antivirus Software** – run antivirus software. Ensure to update the antivirus software along with all other updates and patches.

▢ **Authentication** – enable two-factor authentication for the uploading of results and remote administration of the ENR. Encourage the use of strong passwords and proper password management. Shared passwords should be discouraged. Every account should have its own password and passwords should not be written down or placed in public view.

▢ **Backups** – if at any point there is unexpected activity or the website becomes unavailable it can be restored to the last known state, so that systems and data can be recovered quickly in the event of an incident. Additionally, if a printed copy (electronic or hardcopy) of the results is obtained during the backup process the printed copy can be provided in the interim, until the ENR system is back up and available. The backup and restore process should be tested and validated.

▢ **Communications Security** – use encryption and data integrity to protect communications over any network. In particular Transport Layer Security (TLS) to protect traffic between the client (e.g. web browser) and the server (ENR system).

▢ **Detection** – use an intrusion detection system and monitor the incoming and outgoing traffic for signs of irregularities, such as above average traffic, 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.

▢ **Incident Response Plan** – have an Incident Response Plan in place. Know how you and your jurisdiction would respond to incidents that compromise the availability or integrity of the ENR system.

▢ **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, catalogue the media. This provides an archive of the results uploaded to the ENR system.

▢ **Proof** –verify the data being posted to the ENR system match the official results from the voting system. Validate that the results shown on the website match the official results 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. 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.

▢ **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** – outdated software is the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

Conclusion: Even though the official election results are certified based on the reports from the voting system that has been tested and certified, Election Night Reporting systems provide unofficial results that the public does not necessarily perceive as unofficial. Therefore, providing assurance to the public that the Election Night Reporting system data is accurate and protected is of the utmost importance to every election official. Election officials may use this list as a baseline to assess the current security protocol surrounding the Election Night Reporting system. Also, don't forget to include Election Night Reporting systems in your Continuity of Operations and Risk Management Plans, as well.

Resources: For additional technical resources, reference the following documents.

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52r1, Guidelines for the Selection, Configuration, and Use of TLS Implementations
- NIST SP 800-63-2, Electronic Authentication Guideline
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems
- NIST SP 800-41r1, Guidelines on Firewalls and Firewall Policy
- NIST SP 800-61r2, Computer Security Incident Handling Guide
- Department of Homeland Security (DHS) Best Practices for Continuity of Operations (https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01) (Handling Destructive Malware) (https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01)
- Ransomware: What It Is and What To Do About It

Document assets

☐	Checklist_Securing_ENR-Systems_10.14.16.pdf	509.61 KB

Tags:
Data (/Taxonomy/Term/328), Election Administration (/Taxonomy/Term/83), Security (/Taxonomy/Term/192)