NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Election Security Series

DATA INTEGRITY AND RECOVERY

Overview

Ransomware and other destructive attacks can paralyze a state or local election office, disrupting the vital data records and systems relied upon to prepare for and conduct elections. Even environmental disaster or equipment failure could seriously impair election activities. To ensure the integrity and availability of our election systems, it is essential to protect data assets and be able to restore compromised data quickly after an event. This guide provides an overview of how to identify and protect against data integrity events and how to implement strategies to recover from those incidents, maintain operations, and ensure the integrity of data critical to the election infrastructure.

WHAT IS DATA INTEGRITY AND RECOVERY?

Data integrity and recovery refers to the capabilities, processes, and procedures used to defend against unauthorized data corruption, modification, and destruction. It includes:

- Identifying the critical data assets that may become targets of data integrity attacks and any vulnerabilities that facilitate these attacks
- Protecting these assets against the threat of data corruption and destruction using access control, secure storage, and vulnerability management
- Identifying and recovering from such attacks using integrity monitoring, logging, backups, contingency planning and incident response

HOW TO IMPLEMENT DATA INTEGRITY AND RECOVERY

Election officials should help ensure data integrity and recovery by establishing processes and procedures to:

- **Inventory critical assets—**Identify and inventory devices, data, and applications that may become targets of data integrity attacks. Prioritize these assets based on their criticality to election activities.
- **Safeguard critical data—**Limit access to critical assets through access controls and multi-factor authentication. Keep critical data in secure storage, protected against environmental damage, system failures, user errors and malicious actors. Identify and remediate system vulnerabilities that could lead to a loss of data integrity or system availability.
- **Monitor and log—**Log access to high-value data. Monitor, log, and report changes to critical data assets. Detect and report data corruption. Correlate cybersecurity attacks with all logged events. Analyze logs to detect anomalies in user activity and information. Enable file integrity protection for log files and audit data.
- **Backup data—**Create backups of election records and data, physical and virtual systems, and con-figuration

files on a regular basis so that data can be restored quickly if incidents occur. Protect backups by encrypting media and storing it in secure locations. Test the backup and restoration processes periodically to ensure data and systems can be restored.

- **Contingency planning and incident response—** Develop plans for responding to and recovering from data integrity events. Test contingency plan activities to validate recovery capabilities and to prepare staff for incidents. Plans should be updated regularly to remain current with system enhancements and organizational changes.

HOW DATA INTEGRITY AND RECOVERY SUPPORT CYBERSECURITY OBJECTIVES

Implementing data integrity and recovery measures can help prevent malicious actors from corrupting critical election data and interfering with the election process. When incidents do occur, these measures can help facilitate quick recovery, thereby mitigating potential interference with election systems. The recommendations in this guide can help address the broad range of risks to the integrity of a voting system identified in the **Voluntary Voting System Guidelines 2.0**. These recommendations also help achieve **NIST Cybersecurity Framework** outcomes supporting data integrity—identifying assets (Subcategories ID.AM-1, ID.AM-2), protecting critical data (ID.RA-1, PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, PR.PT-4), monitoring (PR.DS-6, PR.IP-1, PR.PT-1, DE.CM-1), data backups (PR.IP-4), and contingency planning and response activities (ID.RA-2, PR.IP-9, PR.IP-10, DE.AE-4).

Important Resources

- **Voluntary Voting System Guidelines 2.0** – a set of voluntary guidelines from the Election Assistance Commission for voting systems to meet standards for basic functionality, accessibility, and security.
- **NIST Cybersecurity Framework** – a voluntary framework, based on existing standards, guidelines, and practices, for reducing cybersecurity risks to critical infrastructure.
- **NIST Special Publication (SP) 1800-25, Data Integrity Identifying and Protecting Assets Against Ransomware and Other Destructive Events** – a cybersecurity practice guide, developed by NIST's National Cybersecurity Center of Excellence (NCCoE), that demonstrates a practical solution for identifying and protecting against data integrity attacks.
- **NIST SP 1800-11, Data Integrity Recovering from Ransomware and Other Destructive Events** – a cybersecurity practice guide, developed by NIST's NCCoE, that demonstrates a practical solution for monitoring, detecting, and recovering from a data corruption event.
- **NIST SP 800-34, Contingency Planning Guide for Federal Information Systems** – guidelines to implement interim measures to recover information system services after a disruption.

To view other guides in the NIST Election Security Series, visit: vote.nist.gov