

NIST Election Security Series

IMPLEMENTING MULTI-FACTOR AUTHENTICATION

Overview

Our election infrastructure remains a target for malicious actors. Many attacks begin with stolen user credentials, which may give the attacker access to election systems— and with that access, the potential to disrupt elections or undermine public confidence in them. These credentials are often obtained through phishing or brute force attacks, such as password guessing. **Multi-factor authentication (MFA)** is a powerful tool to prevent many of these attacks. This guide provides an overview on how to deploy MFA to protect the election infrastructure.

WHAT IS MULTI-FACTOR AUTHENTICATION?

MFA is a mechanism to verify an individual's identity by requiring them to provide more than just a username and password. MFA requires a user to provide two or more of the following:



- **Something the user knows** – e.g., a password, pass phrase, or personal identification number (PIN)



- **Something the user has** – e.g., a physical token or a phone-based authenticator



- **Something the user is** – e.g., a biometric,

such as a fingerprint or retina pattern

For example, a user could insert a physical hardware token (first factor) into the system and then type in a memorized password (second factor). If the token is stolen or lost, someone who gains possession of it could not log into the system without the password. Conversely, if the password is compromised, someone who learns it could not access the system without the physical token.

HOW TO IMPLEMENT MFA

Below are some steps election officials should consider when implementing MFA:

- **Review systems and applications.** Take inventory of all systems and applications used within the election infrastructure, particularly any public-facing applications (e.g., voter registration sites). What type of authentication (e.g., password, token, biometric) is currently used for each system/application?
- **Choose an appropriate authenticator.** Prioritize implementing MFA on systems/applications that provide access to sensitive data or administrative functions; choose MFA mechanisms that are both secure and usable.
- **Consider organization-wide single sign-on.** Single sign-on systems support secure, centralized identity management and improve usability by enabling users to access multiple applications/systems after presenting their credentials.
- **Manage access to systems.** Ensure that only authorized users have access to relevant systems, and limit or remove access as needs change, such as when a user leaves the organization. Flag or lock accounts when suspicious behavior is detected. Consider technologies that display account activity to spot malicious attacks early.

HOW MFA SUPPORTS CYBERSECURITY OBJECTIVES

Using MFA can help prevent malicious actors from gaining access and possibly interfering with election systems. The recommendations in this guide can help satisfy the access control principle of the **Voluntary Voting System Guidelines 2.0**, which states “the voting system

authenticates administrators, users, devices, and services before granting access to sensitive functions.” These recommendations also help support **NIST Cybersecurity Framework** guidance on protecting networked systems and providing access control to key functions within the network, as described in Subcategories PR.AC-1, PR.AC-6, and PR.AC-7.

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 1800-17, Multifactor Authentication for E-Commerce](#) – a cybersecurity practice guide, developed by the NIST’s National Cybersecurity Center of Excellence, that demonstrates a practical solution for implementing multi-factor authentication.
- [NIST Special Publication 800-63-3, Digital Identities Guidelines](#) – guidelines for identity proofing and authentication of users interacting with government IT systems over open networks.

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