

# 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 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



### HOW TO IMPLEMENT MFA

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

-  **Review current systems and applications –** Take inventory of all systems and applications used within the election infrastructure and the types of authentication mechanisms they use.
-  **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 or when suspicious behavior is detected.



### HOW MFA SUPPORTS CYBERSECURITY OBJECTIVES

The recommendations in this guide can help satisfy the access control principle of the **Voluntary Voting System Guidelines 2.0** and help achieve the desired access control outcomes from the **NIST Cybersecurity Framework**.

### IMPORTANT RESOURCES

- [Voluntary Voting System Guidelines 2.0](#)
- [NIST Cybersecurity Framework](#)
- [NIST Special Publication 1800-17, Multifactor Authentication for E-Commerce](#)
- [NIST Special Publication 800-63-3, Digital Identities Guidelines](#)

For more information on this MFA guide and to view other guides in this series, visit: [vote.nist.gov](https://vote.nist.gov)

