CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

# Multi-Factor Authentication

**Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.**

## Why should State and Local Election Officials be interested in MFA?

Implementing MFA makes it more difficult for an adversary to gain access to secure databases, applications, and other election infrastructure assets. MFA can help prevent adversaries from gaining access to your organization's assets even if passwords are compromised through phishing attacks or other means.

Increasingly, a user ID and password combination alone does not provide enough protection against unauthorized login. One of the major drawbacks of using an ID and password system alone is the requirement to maintain a password database. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. These factors reduce the security of password protected systems and resources more each day.

## How does MFA work?

MFA requires system or network users to present two or more credentials at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- **Something you know:** like a password, Personal Identification Number (PIN), or answers to security questions;
- **Something you have:** like a smart card, mobile token, or hardware token; and
- **Some form of biometric factor** (e.g., fingerprint, voice recognition).

For example, MFA could require users to insert a smart card ID into a card reader (first factor) and then enter a password (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

The added security offered by MFA can simplify the user login process by using single-sign on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time.

Consider deploying an MFA capability to cover voter registration systems, election night reporting systems, or other election office IT systems. Implementation schedules and costs vary depending on the MFA solution your organization chooses and the assets that it covers. These options range from implementing a single sign-on environment to supplementing an existing password-based login system with a second authentication factor, such as a time-limited, single-use code delivered by token or through a smartphone app generator.

2019-03-25