MULTI-FACTOR AUTHENTICATION (MFA)

What is multi-factor authentication (MFA)?

A key security control that provides an enhanced means of verifying the identity of a user by requiring the user to provide two or more authentication factors (i.e., something you know, something you have, or something you are) at login.

Why is MFA important for your institution?

MFA increases the difficulty for threat actors to gain access to information systems via the use of compromised passwords or personal identification numbers (PINs). With MFA implemented, unauthorized users will be unable to access the account without providing a second verification factor. **This added layer of security is a crucial for stopping common malicious cyber activities (e.g., password spraying)**.[1]

- A May 2023 Microsoft study revealed that the use of MFA "reduced the risk of compromise by 99.22% across the entire population and by 98.56% in the case of leaked credentials."[2]
- MFA is not a "magic bullet," nor a substitute for other security controls. However, recent FFIEC guidance on authentication states that, *"When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of layered security can more effectively mitigate risks."*[3]

All MFA is ***NOT*** the same…

For MFA to be most effective, there are three primary considerations:

- ***The type of MFA to be used,***
- ***What assets MFA will be protecting within the organization, and***
- ***How MFA is configured.***

While the use of any form of MFA is preferable to using none, it is important to understand that there are multiple methods of implementing MFA, as well as variations in the degree of security provided by each MFA type.

- **SMS or Voice-Based Authentication** – *relies on codes sent to a user's phone or email*
  - According to CISA, this is the **weakest** form of authentication due to its susceptibility to phishing, exploitation of SS7 vulnerabilities, and SIM swapping. This form of authentication is generally viewed as a **last resort option and a temporary stopgap until stronger authentication methods can be implemented.**
- **Application-Based Authentication Without Number Matching –** *push prompts are received and accepted by a user to approve the request for access with no intermediate steps between the request and acceptance of approval*

---

[1] CISA. *Implementing Phishing-Resistant MFA,* October 2022.

[2] Meyer, L.A., Romery, S., Bertoli, G., Burt, T., Weinart, A., and Ferres, J. (Microsoft Corporation). *How Effective is Multifactor Authentication in Deterring Cyberattacks?* May 2022.

[3] FFIEC. *Authentication and Access to Financial Institution Services and Systems,* August 2021.

- This is a more secure method of MFA; however, this form of authentication is susceptible to push bombing attacks (flooding a user's device with access approval requests) and user error.

- **Application-Based Authentication Using One-Time Passwords (OTP), Mobile Push Notifications with Number Matching, or Token-Based OTP –** *requires an additional step(s) by the user (often the input of a one-time number).*
  - These methods provide an even higher degree of security for the authentication process and are **resistant** to push bombing attacks; however, these methods remain vulnerable to phishing attacks.
- **Phishing Resistant MFA –** *includes FIDO or WebAuthn authentication and public key infrastructure (PKI) implementations*[4]
  - The "**gold standard**" for MFA. CISA urges system administrators and high-value targets to begin implementing or planning their migration to phishing resistant MFA.

***WHERE* you use MFA and *HOW* you configure it matters….**

Like all other security controls, **where you use MFA** and **how it is configured** are important considerations. The implementation of MFA can be a complex process that requires careful planning and a phased approach.

"An asset with the weakest method of authentication becomes a potential path to bypass stronger authentication for a system that it is connected to." - CISA

CISA recommends an organization-wide approach when implementing MFA as **it is more effective to implement MFA across all systems and applications instead of implementing redundant, isolated solutions for individual applications.**[5] Further, it is important for management to identify systems in which MFA is not supported and develop plans for upgrading or migrating to systems that support MFA. The institution's risk assessment can help identify and prioritize areas where MFA application is needed. For organizations that elect to forego an organization-wide implementation of MFA, the primary areas of focus for implementation of MFA typically include, but are not limited to:

- Privileged access management (PAM) (domain administrative access, application administrative access, etc.)
- VPN/Remote Desktop (RDP) access into the network
- Vendor access into the network
- Access to any cloud-based service (email, mortgage origination, HR platforms, etc.)
- Access to external applications hosting nonpublic information (NPI)
- Situations where customers may be accessing NPI[6]

"To receive the full benefit of an MFA capability, organizations should be sure to implement it across all systems, applications, and resources." - CISA

It is important that the chosen MFA technology is **configured properly, monitored, and supported by other security mechanisms** as part of layered security approach. Misconfigured or improperly managed

---

[4] CISA. *Implementing Phishing-Resistant MFA,* October 2022.
[5] CISA. *Capacity Enhancement Guide: Implementing Strong Authentication,* October 2022.
[6] CSBS. *CSBS Ransomware Self-Assessment Tool for Banks,* October 24, 2023.

MFA can provide a false sense of security and may create unintended weaknesses that may be easily exploited by cyber threat actors.

MULTI-FACTOR AUTHENTICATION (MFA): QUESTIONS BOARD MEMBERS SHOULD ASK

Below are some questions you may ask management to ensure MFA has been appropriately implemented to protect against cyber threats.

1. ***Has multi-factor authentication (MFA) been implemented in the institution? If so, does the institution rely on stronger application-based or phishing-resistant authentication methods (FIDO or public key infrastructure), as opposed to weaker SMS (text) or voice-based authentication?***

   WHY THIS IS IMPORTANT: MFA is a foundational security control that provides an enhanced means of verifying the identity of a system user by requiring the user to provide two or more authentication factors (i.e., something you know, something you have, or something you are) at login. While the use of any form of MFA is preferable to using none, it is important to understand that there are multiple methods of implementing MFA, as well as variations in the degree of security provided by each MFA type. In short, all MFA is not the same.

   - *SMS (text) and voice-based MFA methods are common but are the weakest form of authentication and, according to CISA, should ideally be used only as a temporary solution until stronger methods can be implemented in the institution.*
   - *Stronger authentication methods include authentication via mobile push notification (with or without number matching); one-time passwords; and token-based one-time passwords.*
   - *"Phishing-resistant" forms of MFA such as FIDO or WebAuthn authentication and public key infrastructure (PKI) authentication implementations are the gold standard for authentication and can generally offer superior protections against phishing, "push bombing", and other threats.*

2. ***How has MFA been implemented?***
   - ☐ ***For privileged access management (PAM) (domain administrative access, application administrative access, etc.)***
   - ☐ ***For all users that access any cloud-based service (mortgage origination, HR platforms, etc.)***
   - ☐ ***For cloud email services, such as Microsoft 365 and others***
   - ☐ ***For access to external applications hosting non-public information (NPI)***
   - ☐ ***For VPN/Remote Desktop (RDP) access into the network***
   - ☐ ***For vendor access into the network***
   - ☐ ***For internal service accounts***
   - ☐ ***For customers accessing NPI (e-Banking services, remote deposit capture, etc.)?***

   WHY THIS IS IMPORTANT: MFA is implemented within an organization with a goal of strengthening authentication for critical systems and data, as well as protecting the institution against the use of stolen or "guessed" credentials. CISA recommends an organization-wide approach when implementing MFA as it is more effective to implement MFA across all systems and applications

instead of implementing redundant, isolated solutions for individual applications. Further, it is important for management to identify systems in which MFA is not supported and develop plans for upgrading these systems or migrating to new systems where MFA is supported. For organizations who elect to forego an immediate enterprise-wide implementation of MFA, the critical areas of focus for implementation of MFA typically include privileged access management, email and other cloud-based services, applications that host nonpublic information, and remote access (including any vendor access) into the network, among others.

3. ***Does the institution have a plan for future implementation of MFA to protect critical functions and data for areas where it is not currently implemented?***

   WHY THIS IS IMPORTANT: As previously mentioned, CISA recommends taking an organization-wide approach to the implementation of MFA. However, there are a number of factors, such as financial and operational concerns, that can limit an institution's ability to immediately implement an enterprise-wide solution. In these instances, an institution would be well served to carefully evaluate risk and prioritize areas, such as those mentioned above, where MFA implementation is warranted. Due to the potential financial and operational impacts of implementing an MFA solution, it is also advisable that the institution appropriately plan for implementation throughout critical areas via budgeting and strategic planning efforts.

4. ***Are MFA applications properly configured, monitored, and supported by other security mechanisms to afford expected protection?***

   *WHY THIS IS IMPORTANT: MFA is not a "magic bullet", nor a substitute for other security controls when sensitive information is being protected. Recent FFIEC guidance on authentication states that, "When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of **layered security** can more effectively mitigate risks." When MFA is implemented, it is important that the chosen technology is **configured properly, monitored, and supported by other necessary security mechanisms as part of a layered security approach**. Misconfigured or improperly managed MFA applications can provide a false sense of security to the institution and may create unintended weaknesses that may be easily exploited by cyber threat actors.*