Enabling Supply Chain Resilience

Last updated: May 2024

RTX created this supplier cyber enablement series to help our partners reduce and minimize risk by promoting information sharing, raising awareness, and identifying available resources and services.

As part of this series, we're highlighting the Defense Industrial Base (DIB) Sector Coordinating Council (SCC) task force's Top 10 Cyber Best Practices to promote cyber resiliency.

- Enable Multi-Factor Authentication
- Reduce Administrative Rights
- Install and Update Anti-virus/Malware
- Eliminate Default Passwords
- Utilize DNS Mitigations
- Conduct Email Filtering
- Provide Training & Awareness
- Conduct Patching
- Perimeter Hardening
- Web Content Filtering

The focus of this note is ***multi-factor authentication*** (MFA). A recent review of DIB company's supplier cyber incidents indicated that 95% of incidents could have been avoided and mitigated by enforcing MFA. Implementing and enforcing MFA is more than a compliance requirement for the DIB, it is one of the most critical controls in protecting your company's network and intellectual property.

What is MFA and why should it be implemented?

MFA is an authentication method that requires users to provide two or more verification factors to gain access to a resource such as an application or email account. Users will have to identify themselves by more than just a username and password, such as with the addition of an RSA token, Duo, Smartcard, YubiKey or via biometrics.

Passwords can be compromised via social engineering or phishing. Threat actors will look to exploit the credentials of users who create weak passwords and/or reuse passwords across systems. Enforcing MFA is the most effective way to prevent unauthorized access, even when credentials are compromised.

Is MFA a requirement for suppliers?

Subcontractors supporting RTX Department of Defense prime contracts that store, transmit and/or process controlled unclassified information (CUI) have the contractual and regulatory requirement to enforce MFA on their systems to protect CUI as part of their DFARS 252.204-7012 and NIST SP 800-171 (requirement 3.5.3) compliance.

Where should MFA be implemented?

MFA should be implemented where technically feasible, but we encourage suppliers to take immediate action if they're lacking MFA in these key areas:

- Email infrastructure, whether on-premise or hosted through managed service providers (e.g., Microsoft 365).
- External/remote access to their environment.
- Key cloud IT services (IaaS, SaaS and PaaS) containing sensitive data.
- Access to critical systems.
- Administrative level access to systems.

Things to do now:

1. Require MFA for remote network-level access (VPN)
2. Require MFA for remote access to internal tools (WebVPN)
3. Require MFA for elevated privileges
4. Implement MFA on all accounts

Additional resources:

- More information on MFA can be found on the National Defense Information Sharing and Analysis Center (NDISAC) CyberAssist website.
- Detailed instructions on how to implement MFA for Microsoft 365 can be found here.
- More information on can be found on the RTX's Supplier Cybersecurity website.