Remediant

Securing Innovation

Special Update

SecureONE eases path to DFAR 252.204-7012 and NIST SP 800-171 Compliance

Remediant

DFARS 252.204-7012 & NIST SP 800-171: Increasing Security Through Compliance

In November 2013, the US DoD published DFARS 252.204-7012, concering the safeguarding of Unclassified Controlled Technical Information. Later, in August 2015, DoD published the interim rule on Safeguarding Covered Defense Information. In short, this rule change mandated the adherence to the information security protections laid out in NIST SP 800-171 whenever a US DoD Contractor (and, similarly, any subcontractor) handled "Covered Defense Information". On December 30 2015, the US DoD revised this interim rule by changing the due date for implementation of NIST SP 800-171 to December 31, 2017.

November 18 2013: DFARS 252.04-7012 requires protecting UCTI using NIST SP 800-52 controls

June 2015: NIST SP 800-171 is first published.

August 26 2015: US DoD creates DFARS 252.204-7008, titled Compliance with Safeguarding Covered Defense Information Controls, which mandates adherence to the NIST SP 800-171 standard for "Covered Defense Information". See Federal Register 80/165 from August 26, 2015.

December 30 2015: US DoD extends the deadline for adherence to NIST SP 800-171 to December 31, 2017. See Federal Register 80/250 from December 30, 2015.

Covered Defense Information: A New Term, and New Protections, for Old Data

In establishing NIST SP 800-171 as the requirement for protecting CDI, the DoD acknowledged the likely impact:

> *DoD expects that this interim rule may have a significant economic impact on a substantial number of small entities… This rule will apply to all contractors with covered defense information transiting their information systems. DoD estimates that this rule may apply to 10,000 contractors and that less than half of those are small businesses.*
> *--Federal Register / Vol. 80, No. 165 / Wednesday, August 26, 2015*

The DoD stated that most entities that were already in compliance with NIST SP 800-53 would largely be required to make only policy-based updates. However, new protections, in the form of control 3.5.3, would require bringing multi-factor authentication to information systems that contain CDI.

CDI Definition:

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Key Takeaways

- NIST SP 800-171 compliance deadline is December 31, 2017
- New term, CDI, is introduced
- Entities already compliant with NIST SP 800-53 will have policy changes
- Control 3.5.3 introduces MFA mandate

Remediant

Multifactor Authentication: Deep Dive on control 3.5.3

There are 110 controls in NIST SP 800-171, which range in technical complexity from basic to advanced. Amongst the most technically challenging to comply with, control 3.5.3 (and the related control, 3.7.5) describes the new multifactor authentication requirement.
This control has its origins in controls IA-2 ("Identification and Authentication") and AC-6 ("Least Privilege") of NIST SP 800-53, both of which address privileged access.

The DoD recognizes the difficulty of implementing control 3.5.3, as it is likely the only control, for organizations that were already in compliance with NIST SP 800-53, that would require the installation of new hardware/software. From a DoD FAQ released in January 2017:

For companies that were compliant with the 2013 Safeguarding of Unclassified Controlled Technical Information DFARS clause with the table of NIST SP 800-53 controls, almost all the additional NIST SP 800-171 requirements can be accomplished by policy/process changes or adjusting the configuration of existing IT. ***With the exception of the multifactor authentication requirement (3.5.3)****, no additional software or hardware is typically required.*

Control 3.5.3

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

multifactor authentication: requires two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

local access: any access to an information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

network access: any access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

privileged account: An information system account with authorizations of a privileged user.

privileged user: a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. [NB: Definition inherited from CNSSI 4009]

Remediant

Deep Dive on control 3.5.3: Protecting Information Systems

Protecting Information Systems that contain CDI, such as CAD systems, document collaboration systems, etc. may require changes to the application's authentication and/or authorization flow to ensure compliance with the NIST SP 800-171 controls. For normal (non-privileged) users, adding multifactor authentication at the Single Sign On layer can meet the requirement, without having to make modifications to the application or applications underlying the information system. Addressed in a FAQ released in January 2017 (emphasis added):

Q43: Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

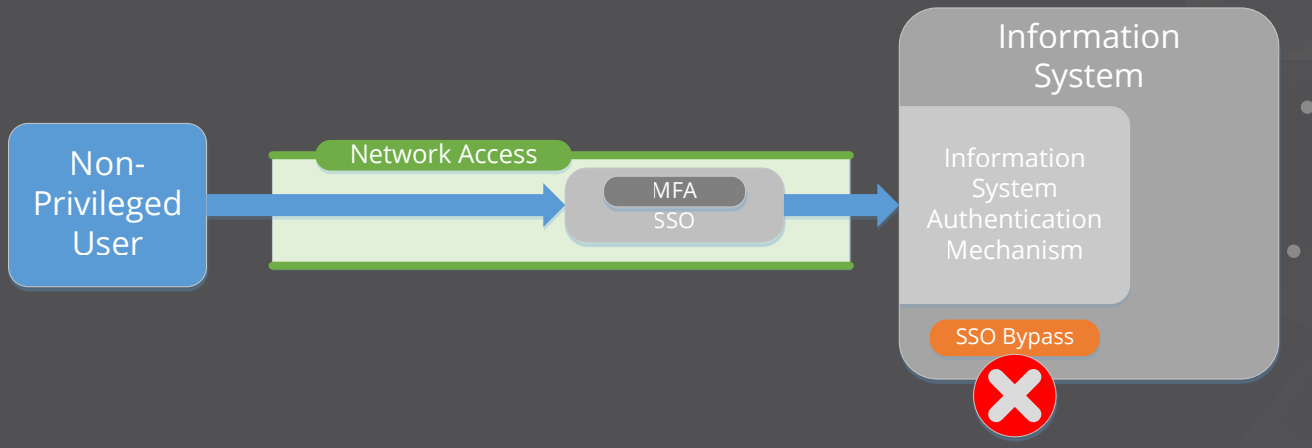
*A43: **The multifactor authentication system is a requirement for local or network access to the information system**, which is different from authentication to a specific information system component (e.g., a router) or an application (e.g., database). While many system components and applications now support (and expect) multifactor authentication, it is not a requirement to implement two-factor authentication on specific devices.*

Information System Definition:

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec 3502)

Adding MFA via SSO

Adding multifactor authentication to an information system that utilizes one of the SSO standards (such as SAML or OAuth) is the easiest path for meeting control 3.5.3, as it relates to normal (non-privileged) user's **network** access. If the information system does not utilize SSO or another standards-based authentication flow, the application underpinning the information system's authentication flow may need to be modified to force multifactor authentication when users authenticate, or when they access CDI within the application. This may require modifying the application itself to change the authentication flow, or adding a separate, interstitial, authentication step before a connection to the information system is made.



Special Note: SSO Bypass

It is important to consider ALL possible access mechanisms. For instance, some applications underpinning the information system may allow bypassing the SSO flow by using a special account and/or a special URL. Multifactor authentication must be applied to all network-based authentication paths that can result in the authenticated user – privileged or non-privileged – having access to CDI. Be sure to look for SSO bypass URLs and accounts, and ensure that they are either closed entirely, or an interstitial login (with MFA) is forced before permitting access to the SSO bypass pages/accounts.

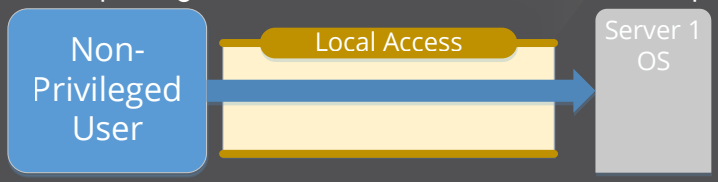
Remediant

Deep Dive on control 3.5.3: Privileged Access Considerations

Control 3.5.3 requires multifactor authentication for local access when privileged accounts are used with an information system. Control 3.7.5 has additional requirements for multifactor authentication when performing maintenance on a system with CDI.

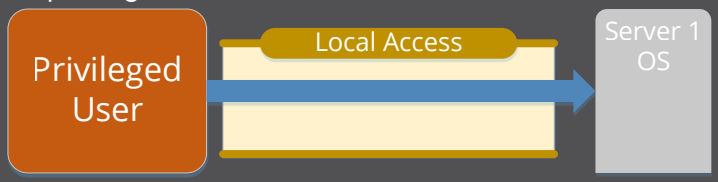
Examples of Local Access:
- A physical keyboard attached to a physical server
- A virtual machine from a local hypervisor
- Local login to industrial control system

Example 1: A non-privileged user has local access. No MFA is required as there is no privileged access in use.



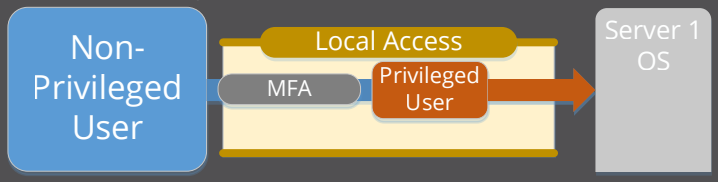
Compliant: No MFA required (assuming NAC is in place)

Example 2: A privileged user has local access to a server without MFA: this is not compliant with control 3.5.3.



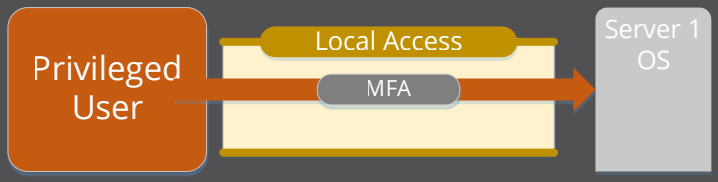
Not compliant: MFA is required

Example 3: A non-privileged user with local access to a server completes multifactor authentication using their non-privileged account. Later, they need privileged access, and authenticate (using just a password) with the separate, privileged, account in order to perform a privileged function on the server. This is not in compliance with control 3.5.3, as the privileged user's account needs to perform both factors of the MFA.



Not compliant: MFA step must be completed using the privileged account

Example 4: A privileged user authenticates using MFA and performs privileged actions on a server using their privileged account. This complies with control 3.5.3.



Compliant: MFA required and performed

Special Note: Switching Accounts

The privileged user must be the one to authenticate with multi-factor authentication, where the both factors are tied to the account that has (or can dynamically gain) the privileged access. An administrator performing tasks that require privileged access must have authenticated via multifactor authentication before being able to assume the privileged role. If the user authenticates with MFA using a non-privileged account (account "x") but privileged access is associated with a separate account (account "A-x"), simply entering the password for account A-X when privileged access is needed is not sufficient to meet the requirement.

From the DoD FAQ:
Q46: If a systems administrator has already been authenticated as a normal user using multifactor authentication, does using his administrative password to install software on the system violate the multifactor requirement?

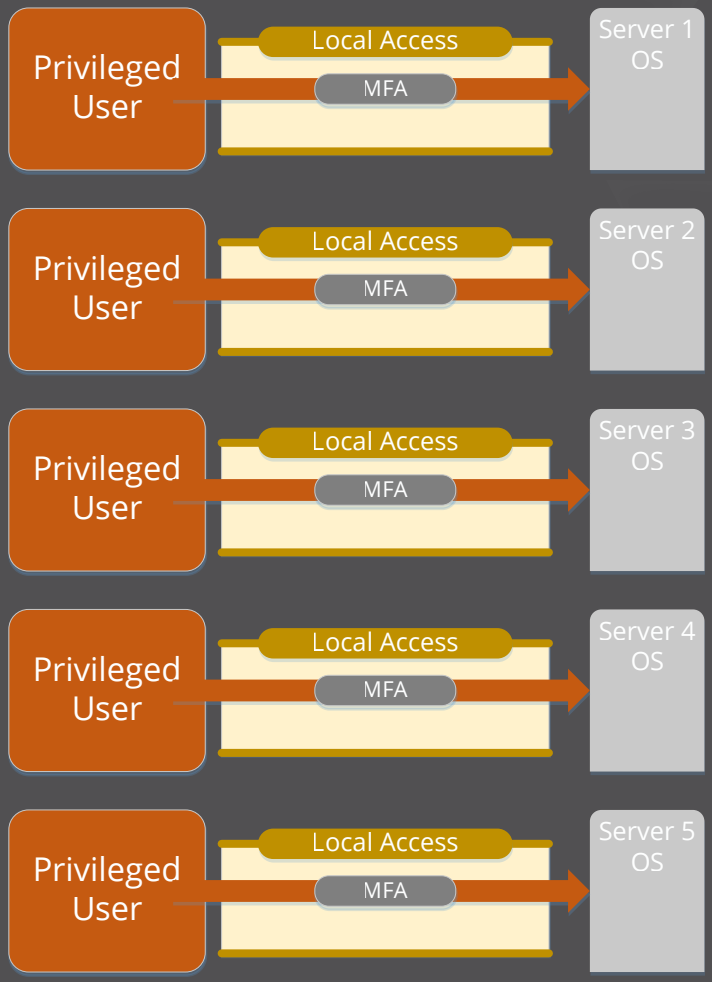
A46: A privileged user (e.g., systems administrator) should always be in the "privileged" role to administer – e.g., he should use multifactor authentication in his privileged role (not as a normal user) to logon to the system to perform administrative functions.

Remediant

Deep Dive on control 3.5.3: Privileged Access 24/7

In environments where administrators have privileged rights persistently (24/7) assigned to their accounts, thus making them privileged accounts, control 3.5.3 requires them to perform multifactor authentication whenever they use those accounts – either locally, or via network access. This may require that the administrator perform MFA many times per day, as their normal duties may require use of those privileged access rights.

Risk: Increased Administrator workload with MFA



Each time a privileged user needs to utilize their privileged access on a system, they must perform their MFA. If an administrator normally logs into several systems per day, or creates/drops sessions several times throughout the day, this will result in significantly increased administrator workload.

However, administrators generally don't need persistent (24/7) privileged access on their accounts. Having broad privileged access not only presents a challenge for NIST SP 800-171 compliance, but also creates a target for malevolent actors to compromise the privileged accounts, and abuse the privileged access rights.

In the next section, we'll discuss a new approach to privileged access rights – Just In Time Privileged Access. By dynamically adding and removing privileged access to an administrator's account, the need to frequently perform multifactor authentication can be lessened – reducing the workload on the administrator and making compliance easier to achieve.

800-171 Control 3.5.3 Summary

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

	Easiest Implementation Path	Alternate Implementation Path(s)
Requirement for network access to information systems: Authenticate all users via multi-factor authentication	Add multifactor authentication to the SSO component of the information system	If the information system does not support SSO or other standards-based authentication schemes, modify it to force MFA when accessing CDI
Requirement for use of local privileged access: Authenticate privileged users via multifactor authentication before they can use privileged access	Implement Just in Time Privileged Access; prompt for MFA once, and then dynamically assign privileged rights when they are needed	Force all users with any privileged access to do MFA whenever they authenticate, since privileged access may or may not be used

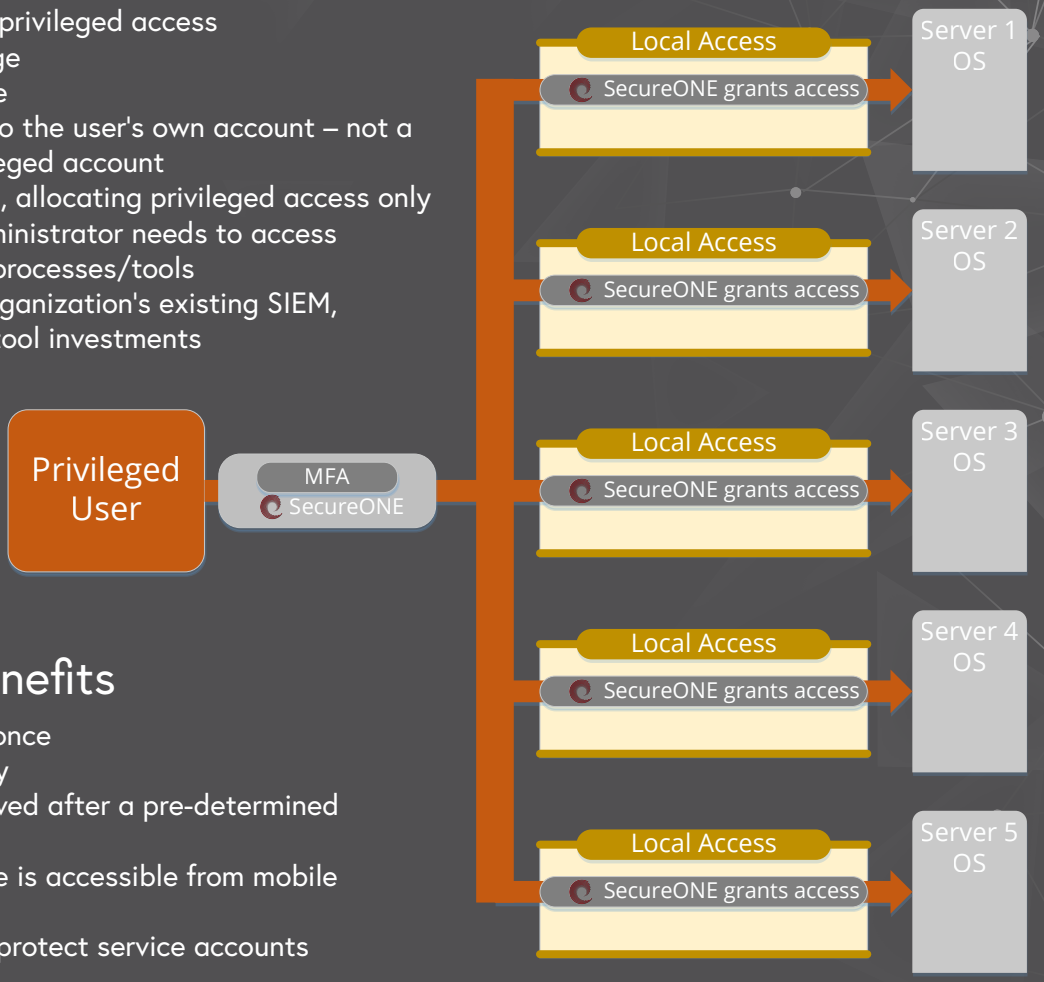
Remediant

Just In Time Administration - A Fresh Approach

With Just In Time Administration, the administrator performs MFA once, and then access rights are granted to their account at the time they need to access each system. Access is then removed when the Privileged User is done performing privileged actions on that system. This approach fulfills the requirements of control 3.5.3, ensuring that MFA is performed for privileged access – whether via network or locally.

Security & Compliance Benefits

+ Meets requirements for 3.5.3 privileged access
+ No agents to install or manage
+ No password vault to manage
+ Privileged access is granted to the user's own account – not a seperate, generic/shared privileged account
+ Follows Least-Privilege model, allocating privileged access only to the specific systems the administrator needs to access
+ Integrates with existing IGA processes/tools
+ Enhances and enriches the organization's existing SIEM, Active Directory and endpoint tool investments



User Experience Benefits

+ Administrators perform MFA once
+ Access is granted dynamically
+ Access is automatically removed after a pre-determined period of time
+ Fully responsive web interface is accessible from mobile devices, desktops and tablets
+ RESTful API makes it easy to protect service accounts

Use Case Examples

There are many ways to utilize the Just In Time Administration technology. Any kind of privileged user can utilize SecureONE, including:

- Server administrators
- IT Service Desk staff
- DevOps Admins
- IT Audit teams
- Service Accounts
- SOC teams
- MSSP users
- Application Support

What is SecureONE and how is it different?

SecureONE is Remediant's next-generation Privileged Access Management product, which provides continuous monitoring for privileged access changes, and makes it easy to enable MFA for privileged access. With SecureONE, administrators only need to perform MFA once, and then SecureONE handles provisioning and deprovisioning the administrator's access to systems on a dynamic basis. If any unexpected privileged changes are detected, a notification is sent to the SIEM and the change is immediately reverted. All of this is accomplished without installing any agents on the endpoints, and without administrators using shared administrator credentials.

Remediant

Securing Innovation

www.remediant.com

info@remediant.com