

June 6, 2023

Shared Responsibilities

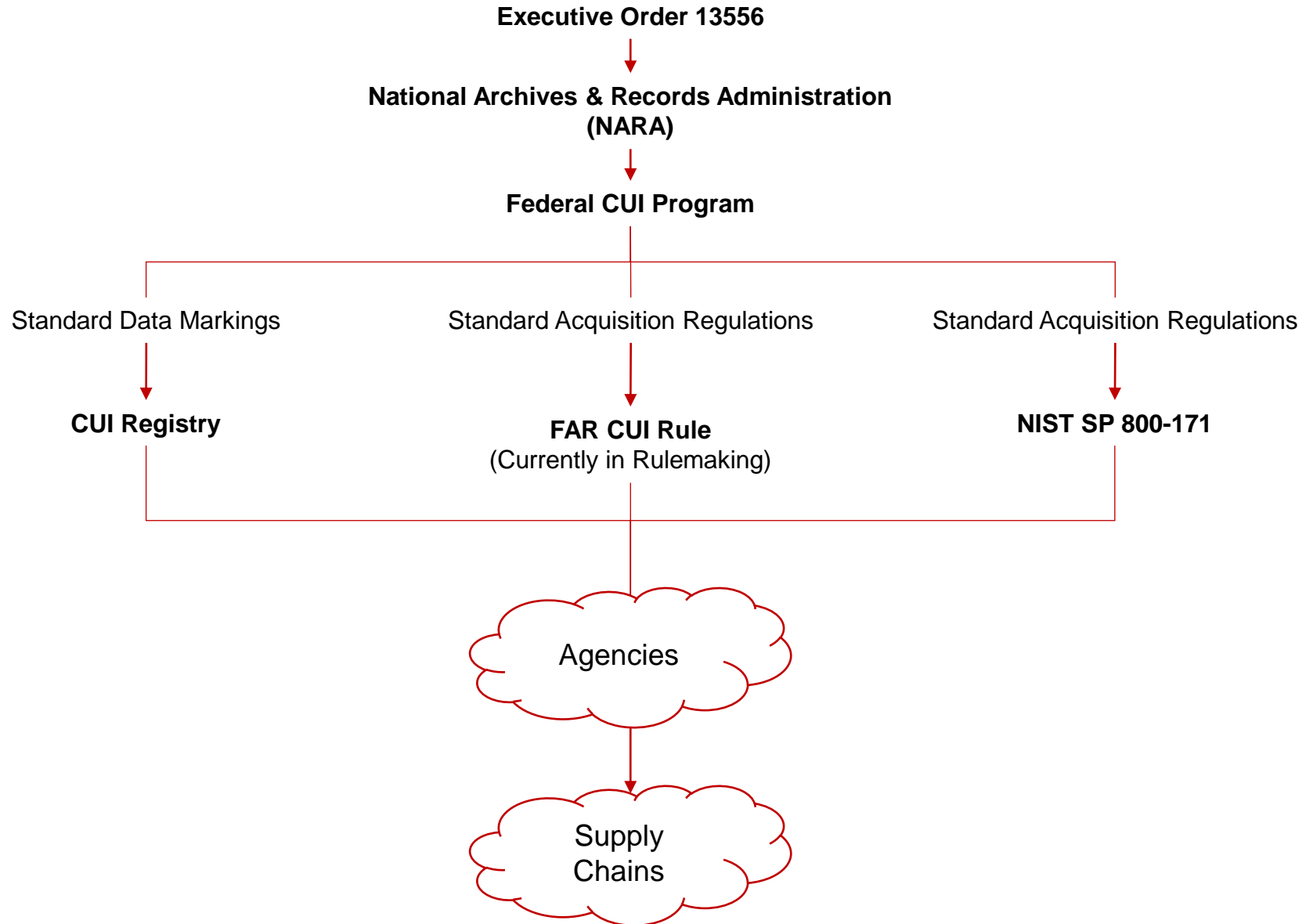
The Role of MSPs in facilitating DFARS, NIST,
and CMMC compliance



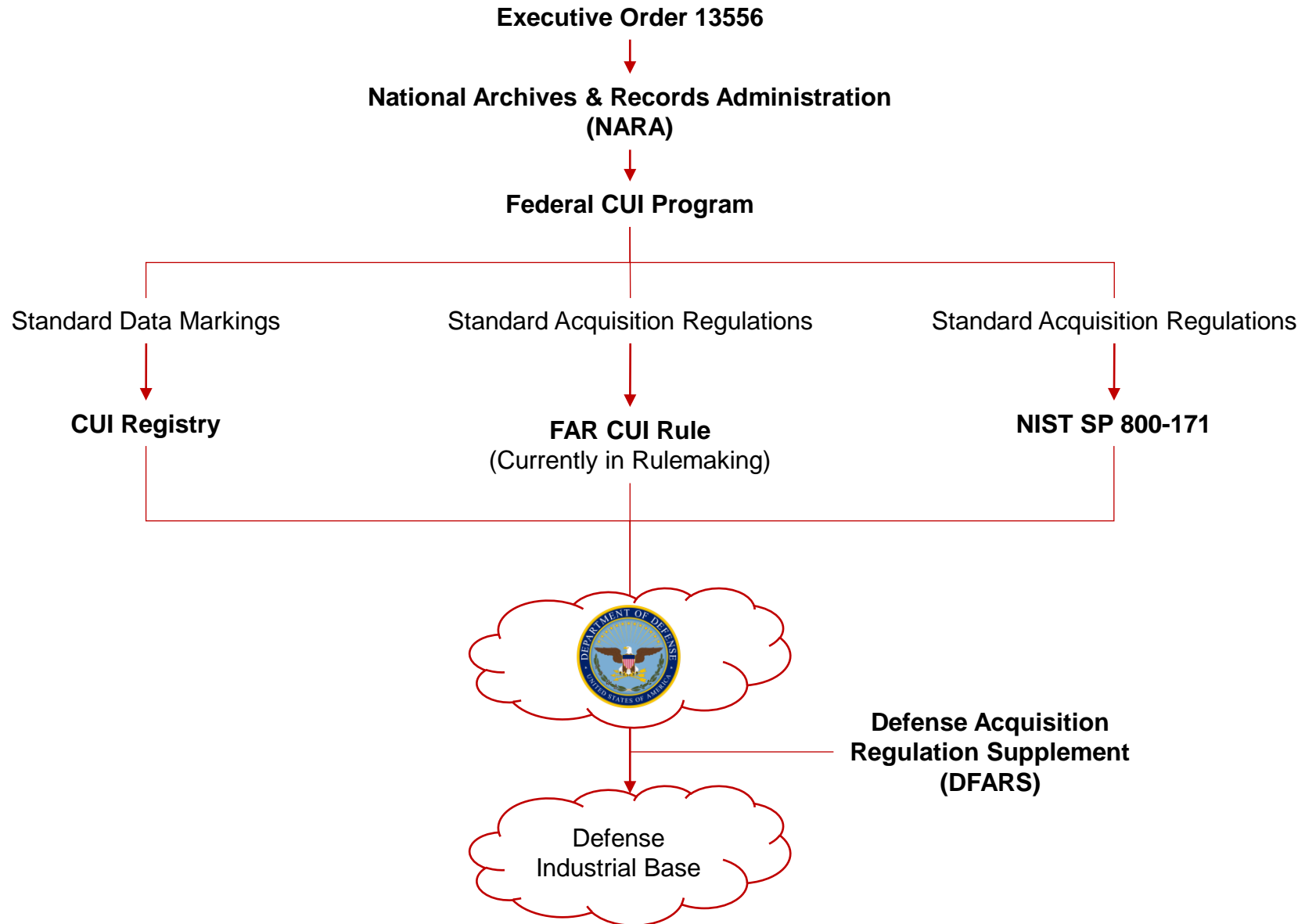
Program vs Requirements

The difference between CMMC and NIST SP 800-171

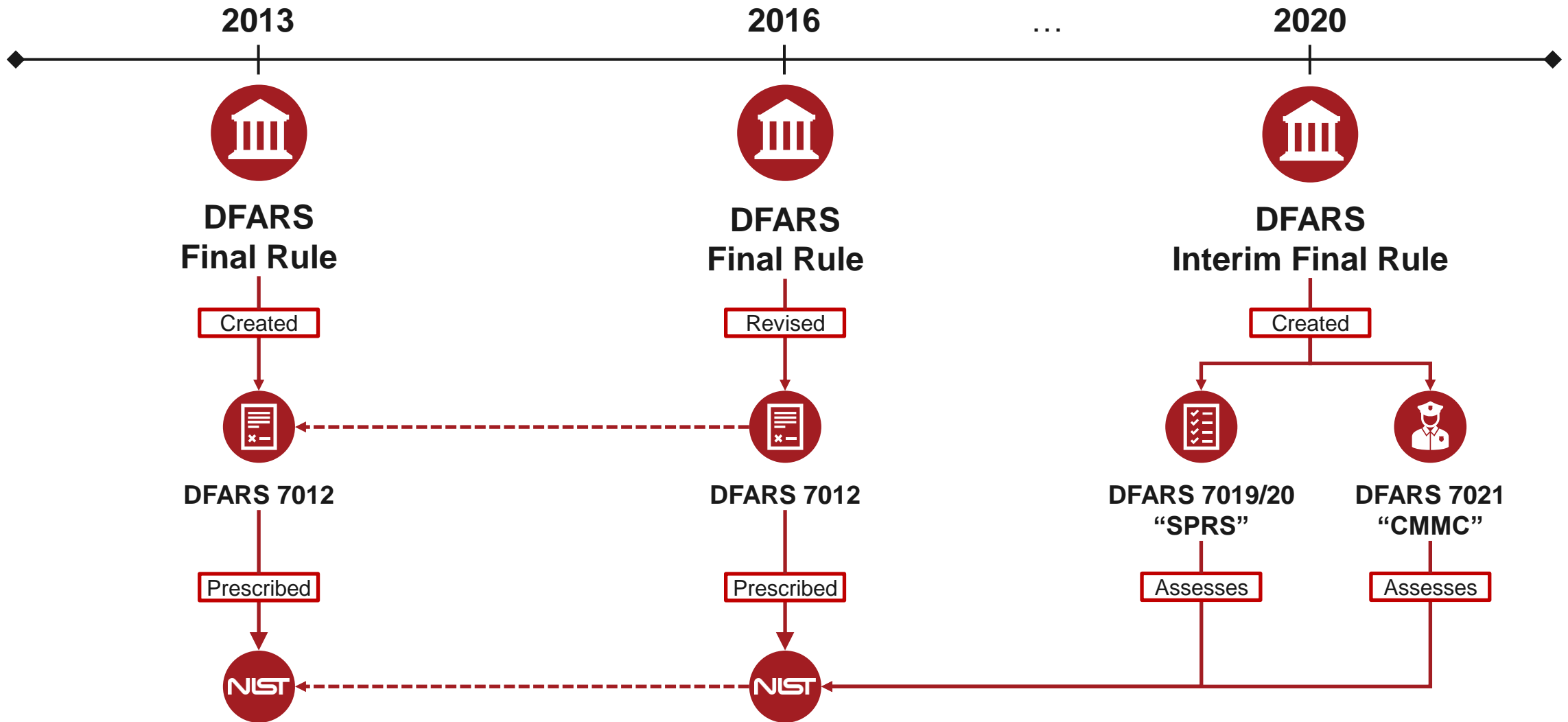
NIST SP 800-171 is a government-wide standard as part of the federal controlled unclassified information (CUI) program



The Defense Federal Acquisition Regulation Supplement (DFARS) extends and enhances Federal Acquisition Regulation (FAR)



Separate rulemaking efforts created separate DFARS cybersecurity clauses

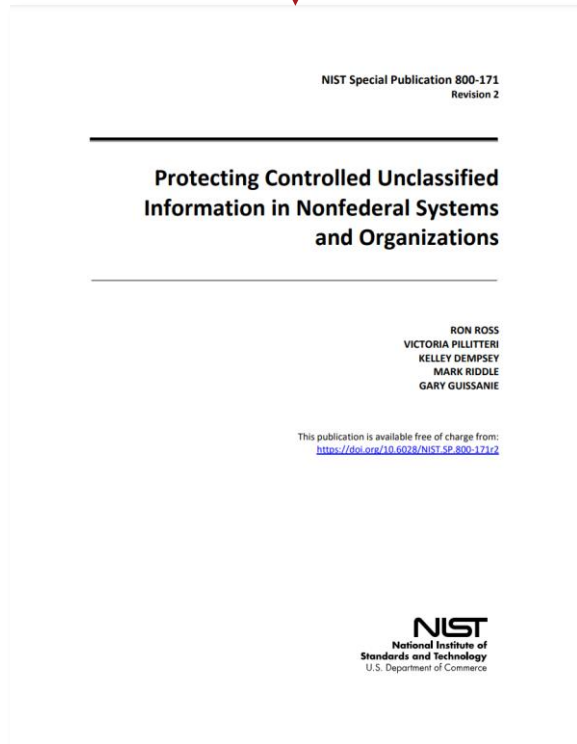


CMMC is a DoD assessment program that verifies if defense contractors have implemented cybersecurity requirements

DFARS 252.204-7012

“Safeguarding Covered Defense Information & Cyber Incident Reporting”

Requires



DFARS 252.204-7021

“Cybersecurity Maturity Model Certification Requirements”

Requires



Assesses

Waiting on the CMMC program to begin implementation of NIST SP 800-171 requirements is a terrible mistake



“NIST SP 800-171 is not part of the discussion as far as our [CMMC] rulemaking is concerned. We all know that’s the requirement that you’re going to have to comply with so that’s not gonna change.”

- Stacy Bostjanick, June 24th, 2022
Chief of Implementation & Policy, DoD Deputy CIO for Cyber

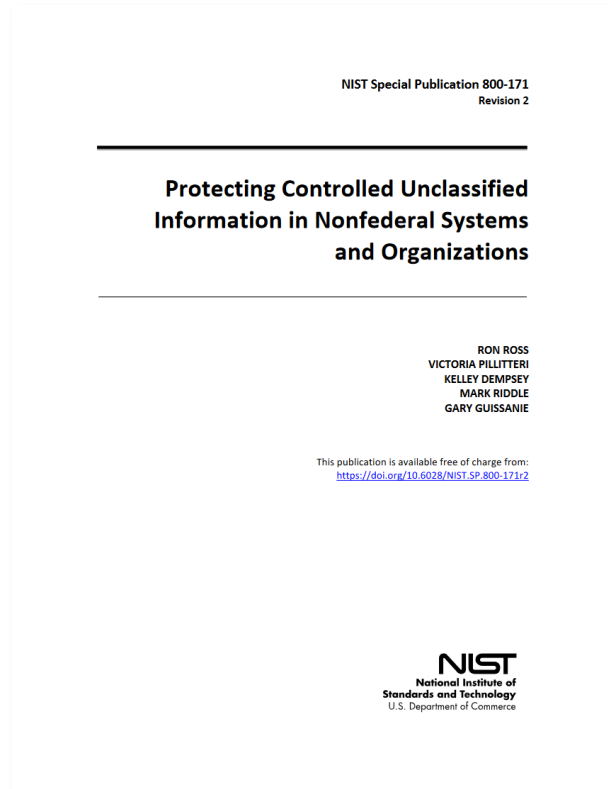


Two Sides of SP 800-171

The relationship between 800-171 and 800-171A

The most important part of NIST SP 800-171 is the part that most people are totally unaware of (NIST SP 800-171A)

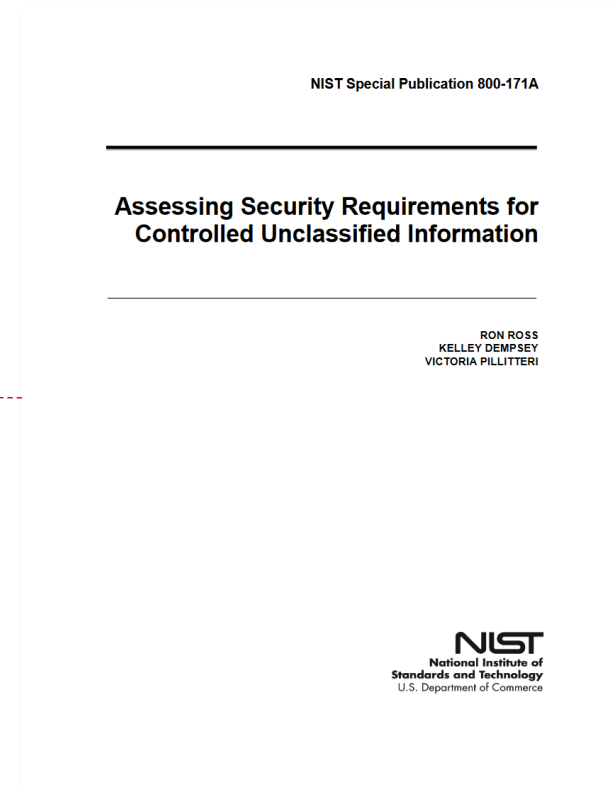
SP 800-171



Defines security requirements

- What to do
- 110 requirements

SP 800-171A



Verifies security requirements

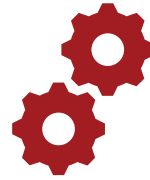
- How to know if you did it
- 320 “determination statements”

SP 800-171A assessment procedures represent the questions that need to be answered in order to verify that a security requirement is fully implemented

How do you **know** if a requirement is...



Properly
Implemented?



Operating as
Intended?



Producing Desired
Outcomes?

For every requirement in SP 800-171 there are multiple “determination statements” that need to be satisfied

SP 800-171

3.1 ACCESS CONTROL

Basic Security Requirements

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged versus non-privileged) are addressed in requirement 3.1.2.

SP 800-171A

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE <i>Determine if:</i>
3.1.1[a]	<i>authorized users are identified.</i>
3.1.1[b]	<i>processes acting on behalf of authorized users are identified.</i>
3.1.1[c]	<i>devices (and other systems) authorized to connect to the system are identified.</i>
3.1.1[d]	<i>system access is limited to authorized users.</i>
3.1.1[e]	<i>system access is limited to processes acting on behalf of authorized users.</i>
3.1.1[f]	<i>system access is limited to authorized devices (including other systems).</i>
	POTENTIAL ASSESSMENT METHODS AND OBJECTS
	Examine: [SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].
	Interview: [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].
	Test: [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

NIST SP 800-171 and SP 800-171A are two sides of the same coin

PUBLICATIONS

SP 800-171 Rev. 2 

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations



Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: [SP 800-171 Rev. 2 \(02/21/2020\)](#)

Planning Note (4/13/2022): 

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The [PDF](#) of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the [CSV](#), [XLSX](#), and the SP 800-171 [PDE](#), please contact sec-cert@nist.gov and refer to the PDF as the normative source.

CUI SSP template

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

[SP 800-171 Rev. 2 \(DOI\)](#)

[Local Download](#)

Supplemental Material:

[Security Requirements Spreadsheet \(xls\)](#)

[Security Requirements CSV \(other\)](#)

[README for CSV \(txt\)](#)

[CUI Plan of Action template \(word\)](#)

[CUI SSP template **\[see Planning Note\] \(word\)](#)

[Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 \(xls\)](#)

Other Parts of this Publication:

[SP 800-171A](#)

Related NIST Publications:

[SP 800-172](#)


Document History:

01/28/21: SP 800-171 Rev. 2 (Final)

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

NIST SP 800-171 and SP 800-171A are two sides of the same coin

PUBLICATIONS

SP 800-171A 

Assessing Security Requirements for Controlled Unclassified Information



Date Published: June 2018

Planning Note (4/13/2022): 

The assessment procedures in SP 800-171A are available in multiple data formats. The [PDF](#) of SP 800-171A is the authoritative source of the assessment procedures. If there are any discrepancies noted in the content between the [CSV](#), [XLSX](#), and the SP 800-171A [PDF](#), please contact sec-cert@nist.gov and refer to the PDF as the normative source.

[CUI SSP template](#)

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Kelley Dempsey (NIST), Victoria Pillitteri (NIST)

DOCUMENTATION

Publication:

[SP 800-171A \(DOI\)](#)

[Local Download](#)

Supplemental Material:

[Assessment Procedures Spreadsheet \(xls\)](#)

[Assessment Procedures CSV \(other\)](#)

[README for CSV \(txt\)](#)

[CUI SSP template **\[see Planning Note\] \(word\)](#)

[CUI Plan of Action template \(word\)](#)

Other Parts of this Publication:

[SP 800-171 Rev. 2](#)

Related NIST Publications:

[ITL Bulletin](#)

Document History:

11/28/17: [SP 800-171A \(Draft\)](#)

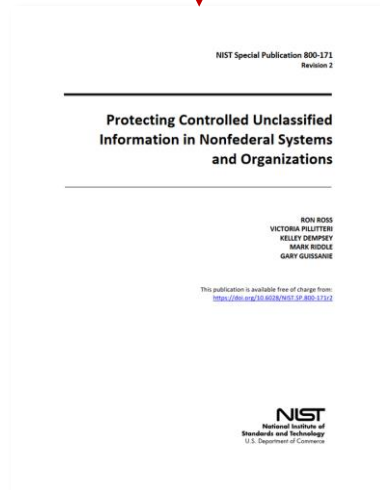
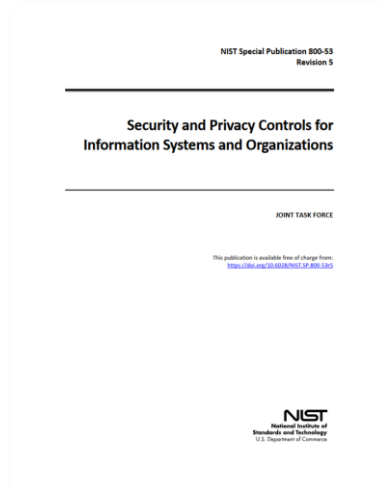
02/20/18: [SP 800-171A \(Draft\)](#)

06/13/18: [SP 800-171A \(Final\)](#)

<https://csrc.nist.gov/publications/detail/sp/800-171a/final>

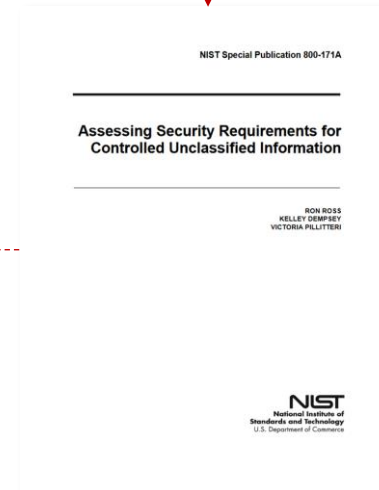
SP 800-171 and 171A are “tailored” from SP 800-53 and 53A, respectively

SP 800-53



SP 800-171

SP 800-53A



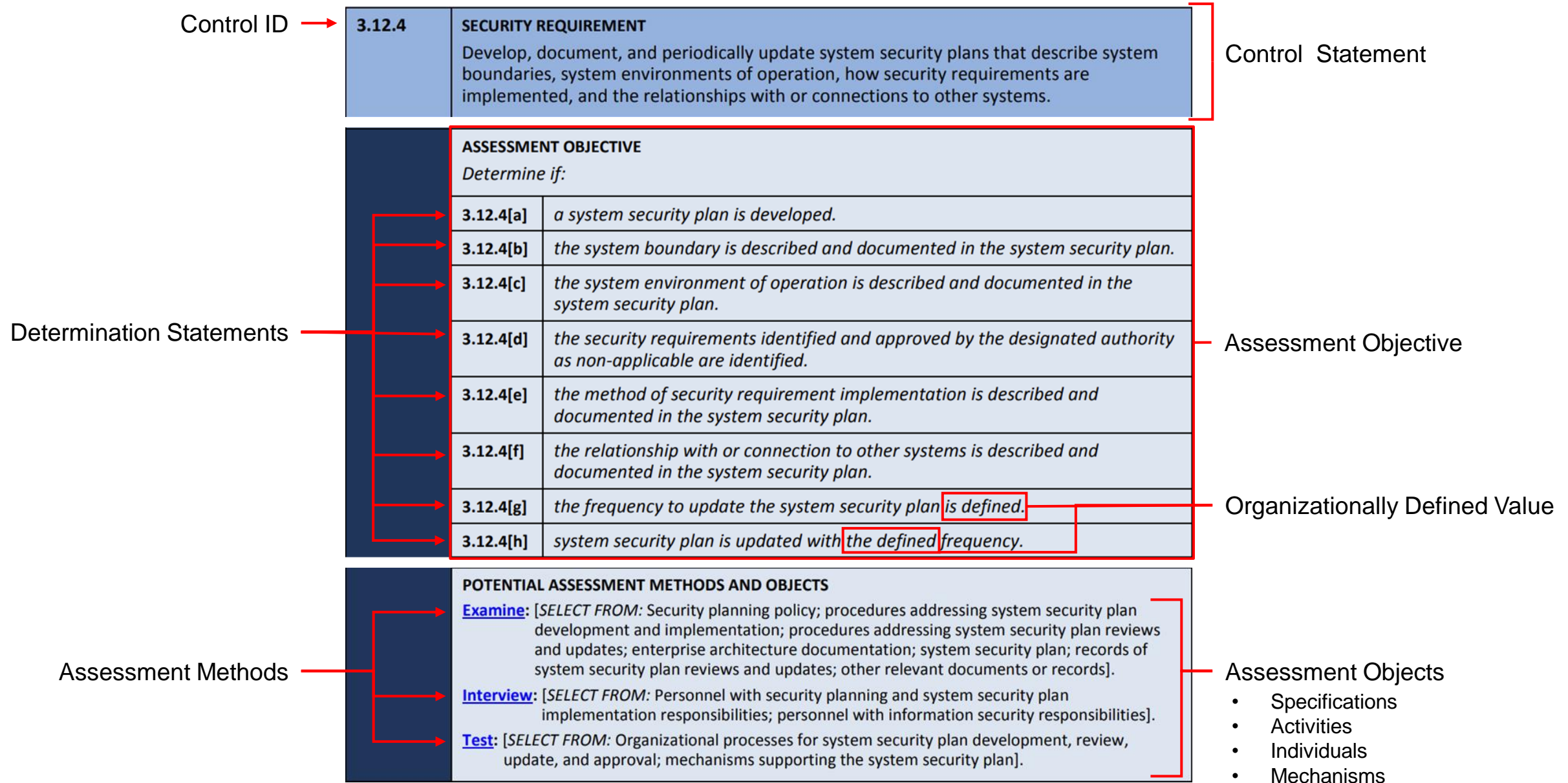
SP 800-171A

An aerial photograph of a city, likely Washington D.C., showing a grid of streets and several large, multi-story buildings. The image is overlaid with a semi-transparent dark blue filter. A white rectangular box is positioned in the center-right of the image, containing the title and subtitle. A vertical red bar is located on the left side of the white box, partially overlapping the city image.

The Philosophy & Anatomy of NIST Controls

Breaking down the components of NIST assessment
procedures

NIST assessment procedures consist of seven major components



The sequence of NIST assessment procedures is not immediately obvious

3.12.4	SECURITY REQUIREMENT Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
	ASSESSMENT OBJECTIVE <i>Determine if:</i>
3.12.4[a]	<i>a system security plan is developed.</i>
3.12.4[b]	<i>the system boundary is described and documented in the system security plan.</i>
3.12.4[c]	<i>the system environment of operation is described and documented in the system security plan.</i>
3.12.4[d]	<i>the security requirements identified and approved by the designated authority as non-applicable are identified.</i>
3.12.4[e]	<i>the method of security requirement implementation is described and documented in the system security plan.</i>
3.12.4[f]	<i>the relationship with or connection to other systems is described and documented in the system security plan.</i>
3.12.4[g]	<i>the frequency to update the system security plan is defined.</i>
3.12.4[h]	<i>system security plan is updated with the defined frequency.</i>
	POTENTIAL ASSESSMENT METHODS AND OBJECTS
	Examine: [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records].
	Interview: [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].
	Test: [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

...about what.

...which questions...

Who gets asked...

NIST controls and assessment procedures reflect a top-down philosophy: management decisions captured as policy are enforced by functionality

3.1.1	SECURITY REQUIREMENT
	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE <i>Determine if:</i>
	3.1.1[a] <i>authorized users are identified.</i>
	3.1.1[b] <i>processes acting on behalf of authorized users are identified.</i>
	3.1.1[c] <i>devices (and other systems) authorized to connect to the system are identified.</i>
	3.1.1[d] <i>system access is limited to authorized users.</i>
	3.1.1[e] <i>system access is limited to processes acting on behalf of authorized users.</i>
	3.1.1[f] <i>system access is limited to authorized devices (including other systems).</i>
	POTENTIAL ASSESSMENT METHODS AND OBJECTS
	Examine: [SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].
	Interview: [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].
	Test: [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

↓

Authorization decisions

- Identify, Specify, Document, Authorize, etc.

System functionality

- Limit, control, monitor, detect, respond, etc.

↑

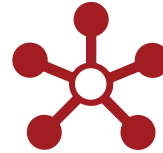
Who gets asked...

“Hybrid” control implementations refer to shared responsibilities across a set of determination statements



“System Specific”

I satisfy all determination statements for this requirement.



“Common Controls”

They satisfy all determination statements for this requirement.



“Hybrid” (“Shared”)

*We** satisfy all determination statements for this requirement.

***See: Appendix A**



The Shared Responsibility Matrix

Properly documenting hybrid control implementations against NIST SP 800-171A

Responsibilities are clear only when they reflect the granularity of SP 800-171A

3.1.1	SECURITY REQUIREMENT
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	

3.1.1(a)	[a] authorized users are identified.			<p>Responsibility: The customer is responsible for developing, implementing, and enforcing the policies and procedures for authorizing users to access the system.</p>
3.1.1(b)	[b] processes acting on behalf of authorized users are identified.			<p>Evidence: Policies and procedures for authorizing users to access the system. Should result in a consistent, repeatable process for developing and managing a "list" of authorized users as the criteria against which this objective is assessed.</p>
3.1.1(c)	[c] devices (and other systems) authorized to connect to the system are identified.			<p>Responsibility: The customer is responsible for developing, implementing, and enforcing the policies and procedures for authorizing processes acting on behalf of authorized users to access the system.</p>
3.1.1(d)	[d] system access is limited to authorized users.	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory to establish managed user accounts. All user account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AAD and evidence of request/authorization from customer for users to be added/removed.</p>	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory (cloud only) as a combination of Active Directory and Azure Active Directory (hybrid) to establish managed user accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AD/AAD and evidence of request/authorization from customer for users to be added/removed.</p>	<p>Evidence: Policies and procedures for authorizing users to access the system. Should result in a consistent, repeatable process for developing and managing a "list" of authorized users as the criteria against which this objective is assessed.</p>
3.1.1(e)	[e] system access is limited to processes acting on behalf of authorized users.	<p>Implementation Summary: Summit 7 provisions process access to the system, utilizing Azure Active Directory to establish managed service or application accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of application/service accounts within AAD and evidence of request/authorization from customer for application/service accounts to be added/removed.</p>	<p>Implementation Summary: Summit 7 provisions process access to the system, utilizing Azure Active Directory (cloud only) as a combination of Active Directory and Azure Active Directory (hybrid) to establish managed service or application accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of application/service accounts within AD/AAD and evidence of request/authorization from customer for application/service to be added/removed.</p>	<p>Responsibility: The customer is responsible for developing, implementing, and enforcing the policies and procedures for authorizing devices to connect to the system.</p>
3.1.1(f)	[f] system access is limited to authorized devices (including other systems).	<p>Implementation Summary: Summit 7 limits connection of device to the system by only joining customer-authorized devices to Azure Active Directory.</p> <p>Evidence: Walkthrough of devices within AAD and evidence of request/authorization from customer for devices to be added/removed.</p>	<p>Implementation Summary: Summit 7 limits connection of device to the system by only joining customer-authorized devices to Azure Active Directory (cloud only) as Active Directory and Azure Active Directory (hybrid).</p> <p>Evidence: Walkthrough of devices within AD/AAD and evidence of request/authorization from customer for devices to be added/removed.</p>	<p>Evidence: Policies and procedures for authorizing devices to connect to the system. Should result in a consistent, repeatable process for developing and managing a "list" of authorized devices as the criteria against which this objective is assessed.</p>

Responsibilities are clear only when they reflect the granularity of SP 800-171A

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
--------------	--

3.1.1(a)	[a] authorized users are identified.		
3.1.1(b)	[b] processor acting on behalf of authorized users are identified.		
3.1.1(c)	[c] devices (and other systems) authorized to connect to the system are identified.		
3.1.1(d)	[d] system access is limited to authorized users.	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory to establish/manage user accounts. All user account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AAD and evidence of request/authorization from customer for user to be added/removed.</p>	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory (cloud only) as a combination of Active Directory and Azure Active Directory (hybrid) to establish/manage user accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AD/AAD and evidence of request/authorization from customer for user to be added/removed.</p>
3.1.1(e)	[e] system access is limited to processor acting on behalf of authorized users.	<p>Implementation Summary: Summit 7 provisions process access to the system, utilizing Azure Active Directory to establish/manage service or application accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of application/service accounts within AAD and evidence of request/authorization from customer for application/service accounts to be added/removed.</p>	<p>Implementation Summary: Summit 7 provisions process access to the system, utilizing Azure Active Directory (cloud only) as a combination of Active Directory and Azure Active Directory (hybrid) to establish/manage service or application accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of application/service accounts within AD/AAD and evidence of request/authorization from customer for application/service to be added/removed.</p>
3.1.1(f)	[f] system access is limited to authorized devices (including other systems).	<p>Implementation Summary: Summit 7 limits connections of device to the system by only joining customer-authorized devices to Azure Active Directory.</p> <p>Evidence: Walkthrough of devices within AAD and evidence of request/authorization from customer for device to be added/removed.</p>	<p>Implementation Summary: Summit 7 limits connections of device to the system by only joining customer-authorized devices to Azure Active Directory (cloud only) or Active Directory and Azure Active Directory (hybrid).</p> <p>Evidence: Walkthrough of devices within AD/AAD and evidence of request/authorization from customer for device to be added/removed.</p>

<p>Responsibility: Summit 7 is responsible for the enforcement of limiting access to authorized users, as identified by the customer via objective [a], within the bounds of the components Summit 7 is contracted to manage on the customer's behalf.</p> <p>Any user access that involves components outside of the scope of the Summit 7 project is the responsibility of the customer to limit accordingly.</p>
<p>Evidence: In addition to the evidence provided by Summit 7 for the components Summit 7 manages, the customer must provide evidence that user access to system components under the customer's control is limited to authorized users IAW policies/procedures.</p>
<p>Responsibility: Summit 7 is responsible for the enforcement of limiting access to processes acting on behalf of authorized users, as identified by the customer via objective [b], within the bounds of the components Summit 7 is contracted to manage on the customer's behalf.</p> <p>Any process access that involves components outside of the scope of the Summit 7 project is the responsibility of the customer to limit accordingly.</p>
<p>Evidence: In addition to the evidence provided by Summit 7 for the components Summit 7 manages, the customer must provide evidence that application/service account access to system components under the customer's control is limited to authorized processes acting on behalf of authorized users IAW policies/procedures</p>
<p>Responsibility: Summit 7 is responsible for the enforcement of limiting connections to the system to authorized devices, as identified by the customer via objective [c], within the bounds of the components Summit 7 is contracted to manage on the customer's behalf.</p> <p>Any device connections that involve components outside of the scope of the Summit 7 project are the responsibility of the customer to limit accordingly.</p>
<p>Evidence: In addition to the evidence provided by Summit 7 for the components Summit 7 manages, the customer must provide evidence that device connections to system components under the customer's control are limited to authorized devices IAW policies/procedures.</p>

Responsibilities are clear only when they reflect the granularity of SP 800-171A

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
--------------	--

AO	Assessment Objectives	Description	Guardian - M365	Guardian - Azure
3.1.1[d]	[d] system access is limited to authorized users.	An assessor will determine whether system access is limited to only the authorized users identified in objective [a].	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory to establish/manage user accounts. All user account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AAD and evidence of requests/authorizations from customer for users to be added/removed.</p>	<p>Implementation Summary: Summit 7 provisions user access to the system, utilizing Azure Active Directory (cloud only) or a combination of Active Directory and Azure Active Directory (hybrid) to establish/manage user accounts. All account provisioning is conducted in accordance with authorization from the customer.</p> <p>Evidence: Walkthrough of user accounts within AD/AAD and evidence of requests/authorizations from customer for users to be added/removed.</p>

An aerial photograph of a university campus, showing various buildings, parking lots, and walkways. The image is overlaid with a semi-transparent dark blue filter. A white rectangular box is positioned in the center-right of the image, containing the main text. A vertical red bar is located on the left side of the white box.

Is This Actually Required?

Yes. It is.

CUI Notice 2020-04: Assessing Security Requirements for CUI in Nonfederal Information Systems

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo



CUI Notice 2020-04: Assessing Security Requirements for CUI in Non-Federal Information Systems

June 16, 2020

Purpose

1. This Notice provides guidance on assessing security requirements for CUI within non-Federal information systems in unclassified environments.

Authorities

2. The Director of the Information Security Oversight Office (ISOO), exercises Executive Agent (EA) responsibilities for the CUI Program. 32 CFR Part 2002, Controlled Unclassified Information, establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.
3. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, establishes security requirements to ensure CUI's confidentiality on non-Federal systems. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, provides procedures for assessing the CUI requirements in NIST SP 800-171 and is the primary and authoritative source of guidance for organizations conducting such assessments.
4. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless an authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the relevant CUI category prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).
5. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance document does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

Assessment Guidance

6. When any entity assesses compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171.
7. The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of safeguards used to meet the security requirements specified in

“NIST SP 800-171A provides procedures for assessing the CUI requirements in NIST SP 800-171 and is the primary and authoritative source of guidance for organizations conducting such assessments.”

“When any entity assess compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls.”

NIST SP 800-171 requirements are an independent variable to programs like CMMC

AC.1.001

Access Control (AC)

Level 1 AC Practices

AC.1.001

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC Assessment Guide - Level 3 | Version 1.10

10

CMMC Assessment Guide v1.10
November 2020

AC.L1-3.1.1 - Authorized Access Control

Access Control (AC)

Level 1 AC Practices

AC.L1-3.1.1 - AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC Assessment Guide - Level 2 | Version 2.0

12

CMMC Assessment Guide v2.0
December 2021

NIST controls and requirements are only “fully implemented” if all determination statements are satisfied

3.12.4	SECURITY REQUIREMENT Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
--------	---

Inflexible

Inflexible	ASSESSMENT OBJECTIVE Determine if:	
	3.12.4[a]	<i>a system security plan is developed.</i>
	3.12.4[b]	<i>the system boundary is described and documented in the system security plan.</i>
	3.12.4[c]	<i>the system environment of operation is described and documented in the system security plan.</i>
	3.12.4[d]	<i>the security requirements identified and approved by the designated authority as non-applicable are identified.</i>
	3.12.4[e]	<i>the method of security requirement implementation is described and documented in the system security plan.</i>
	3.12.4[f]	<i>the relationship with or connection to other systems is described and documented in the system security plan.</i>
	3.12.4[g]	<i>the frequency to update the system security plan is defined.</i>
	3.12.4[h]	<i>system security plan is updated with the defined frequency.</i>

Flexible

Flexible	POTENTIAL ASSESSMENT METHODS AND OBJECTS <u>Examine:</u> [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. <u>Test:</u> [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].
----------	--

NIST controls and requirements are only “fully implemented” if all determination statements are satisfied

RE: 3.12.1 and NIST SP 800-171A



OSD NCR DOD CIO Mailbox DIB CS IA Program Registration <osd.ncr.dod-cio.mbx.dib-cs-ia-program-registration@mail.mil>

To Jacob Horne

Signed By [redacted]ctr@mail.mil

Reply Reply All Forward

Wed 10/20/2021 5:37 AM

Mr. Horne,

Please see below for a coordinated response from the DoD CIO.

You are correct. The ‘assessment objective’ for any particular security requirement is typically made up of several ‘determination statements’ which relate to specific elements of the security requirement. If, upon assessment, any of those determination statements is not met, this results in a finding of ‘other than satisfied’ and the accordingly, the overall security requirement would be assessed as ‘other than satisfied’ until the issue was addressed by the organization, and, per the NIST SP 800-171 DoD Assessment Methodology, the relevant points would be deducted from the overall score of 110. Note that some NIST SP 800-171 allow for a range of values to be deducted, depending on what specific elements of the requirement have not been met.

Please let me know if you have any further questions. Thank you.

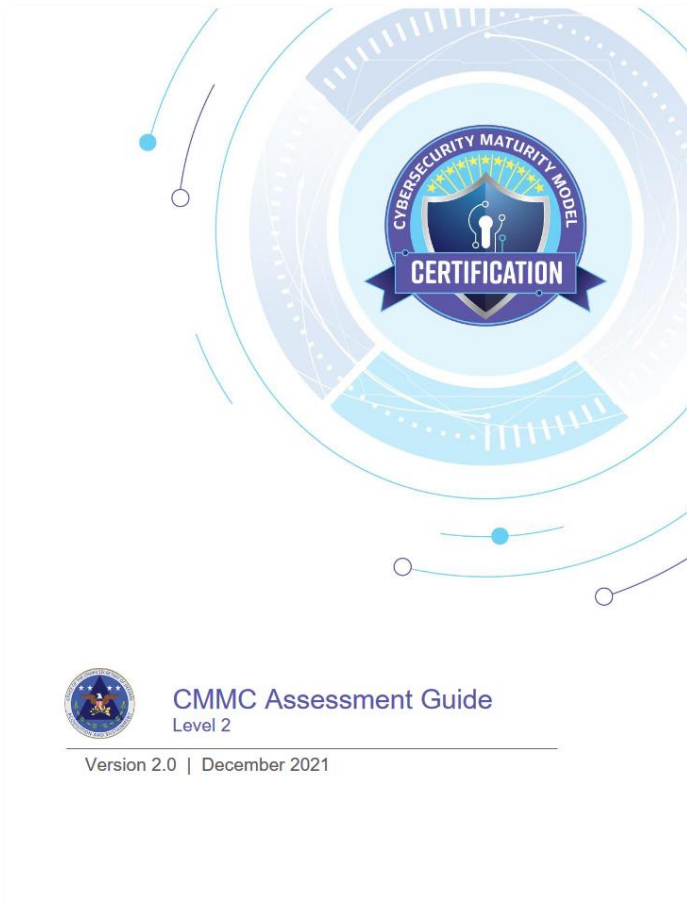
V/r

James

DoD CIO
DIB Cybersecurity Program

C: [redacted]
D: [redacted]ctr@mail.mil

NIST controls and requirements are only “fully implemented” if all determination statements are satisfied



“MET: The contractor successfully meets the practice. For each practice marked MET, the Certified Assessor includes statements that indicate the response **conforms to all objectives** and documents the appropriate evidence to support the response.”

NIST controls and requirements are only “fully implemented” if all determination statements are satisfied



“A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective.”

“Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the **assessment objectives are met.**”

The ability to achieve CMMC certification hinges directly on the quality of the shared responsibility matrix



External Service Provider Considerations

An ESP can be within the scope of applicable CMMC practices if it meets CUI asset criteria. Special considerations for a contractor using an ESP include the following:

- Evaluate the ESP's shared responsibility matrix where the provider identifies security control objectives that are the provider's responsibility and security control objectives that are the contractor's responsibility. In some instances, cloud service providers might expose configuration settings and parameters that the consumer can use to meet CMMC practice objectives.
- Consider the standards that the ESP conforms to and/or what accreditations it has (e.g., FedRAMP, SOC 2, and CMMC Certification).
- Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the contractor's information security objectives.

An aerial photograph of a university campus, showing various buildings, parking lots, and walkways. A white rectangular box is overlaid on the right side of the image, containing the text 'Key Takeaways'. A vertical red bar is positioned to the left of the text box.

Key Takeaways

Key Takeaways

- NIST requirements are an independent variable to CMMC assessments
- NIST SP 800-171A is the center of gravity of gravity, not NIST SP 800-171
- SP 800-171A is much larger and all determination statements must be satisfied for a requirement to be fully implemented
- The structure and philosophy of NIST controls complicates the ability for companies to outsource 100% of their security requirements
- The limits of MSP services and agreements need to be reflected against the granularity of SP 800-171A



Appendix A

Roles & Responsibilities by NIST SP 800-171 Family

3.1 Access Control: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. account management
2. access enforcement
3. defining divisions of and separation of duties
4. defining least privileges necessary to accomplish specified tasks
5. providing legal advice
6. managing remote access connections
7. managing wireless access connections
8. personnel using mobile devices to access organizational systems
9. access control mobile devices
10. defining terms and conditions for use of external systems to access org. systems
11. Restricting/prohibiting use of org.-controlled storage devices on external systems
12. managing publicly accessible information posted on organizational systems

3.2 Awareness & Training: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. security awareness training
2. personnel composing the general system user community
3. role-based security training
4. personnel with assigned system security roles and responsibilities
5. personnel that participate in security awareness training
6. basic security awareness training

3.3 Audit & Accountability: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. audit and accountability
2. audit record review, analysis, and reporting
3. audit record reduction and report generation

3.4 Configuration Management: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. configuration management
2. establishing the system inventory
3. updating the system inventory
4. security configuration management
5. configuration change control
6. members of change control board or similar
7. conducting security impact analysis
8. logical access control
9. physical access control
10. reviewing programs, functions, ports, protocols, and services on the system
11. identifying software authorized or not authorized to execute on the system
12. governing user-installed software
13. operating, using, or maintaining the system
14. monitoring compliance with user-installed software policy

3.5 Identification & Authentication: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. system operations
2. account management
3. authenticator management
4. identifier management

3.6 Incident Response: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. incident handling
2. contingency planning
3. incident response training and operational
4. incident response assistance and support
5. access to incident response support and assistance capability
6. incident monitoring
7. incident reporting
8. personnel who have or should have reported incidents
9. personnel (authorities) to whom incident information is to be reported

3.7 Maintenance: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. system maintenance
2. media sanitization

3.8 Media Protection: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. system media protection
2. system media protection and storage
3. media sanitization
4. system media protection and marking
5. system media transport
6. system media use
7. system backup

3.9 Personnel Security: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. personnel security
2. account management

3.10 Physical Protection: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. physical access authorization
2. physical access to system facility
3. physical access monitoring
4. incident response
5. physical access control
6. personnel approving use of alternate work sites
7. personnel using alternate work sites

3.11 Risk Assessment: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. risk assessment
2. risk assessment, security assessment and vulnerability scanning
3. vulnerability scan analysis
4. vulnerability remediation

3.12 Security Assessment: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. security assessment
2. plan of action development and implementation
3. security planning and plan implementation

3.13 System & Communications Protection: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. boundary protection
2. security planning and plan implementation
3. cryptographic key establishment and management
4. cryptographic protection
5. managing collaborative computing devices
6. managing mobile code
7. managing VoIP

3.14 System & Information Protection: Family-Unique Responsibilities

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Total
SP 800-171 Requirements	22	3	9	9	11	3	6	9	2	6	3	4	16	7	110
SP 800-171A Questions	70	9	29	44	25	14	10	15	4	16	9	14	41	20	320
Responsible for Security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	110
System Administrators	X		X	X	X								X		78
System Developers	X		X	X	X								X		36
Family-Unique Responsibilities	12	6	3	14	4	9	2	7	2	7	4	3	7	9	89

Personnel Responsible for:

1. installing, configuring, and maintaining the system
2. flaw remediation
3. configuration management
4. malicious code protection
5. security alert and advisory
6. implementing, operating, maintaining, and using the system
7. Personnel to whom alerts, advisories, and directives are to be disseminated
8. monitoring the system
9. the intrusion detection system