FERNANDO MACHADO
CISO, CYBERSEC INVESTMENTS

- Cybersecurity Consulting:
  - 10+ years DoD cybersecurity experience
  - NIST 800-171: Controlled Unclassified Information (CUI) / Cybersecurity Maturity Model Certification (CMMC)
  - Army, Navy, Air Force customer experience
- Certified:
  - Certified CMMC Assessor (CCA)
  - Certified CMMC Professional (CCP)
  - Authorized CMMC 3rd Party Assessment Organization (C3PAO)
- Awards:
  - President's Volunteer Service Award

1900 S Harbor City Blvd. Suite 328
Melbourne, Florida 32901

info@cybersecinvestments.com
1-800-960-8802

LinkedIn

CAICO
CERTIFIED CMMC ASSESSOR

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

THE PRESIDENT'S VOLUNTEER SERVICE AWARD

Cybersec
INVESTMENTS

PUBLIC
Public Release Authorized

ACRONYMS

- https://cybersecinvestments.com/2023/07/common-acronyms/

CMMC: UNRAVELED

Cybersec
INVESTMENTS

AGENDA

- CMMC Model
- Common Pitfalls
  - NIST SP 800-171
  - DoD Assessment Methodology
  - DFARS 252.204-7012
  - DFARS 252.204-7019
  - DFARS 252.204-7020
- Top 10 ‘Other than Satisfied’ Requirements
- NIST SP 800-171A / CMMC Assessment Process (CAP)
- Joint Surveillance Voluntary Assessment (JSVA)

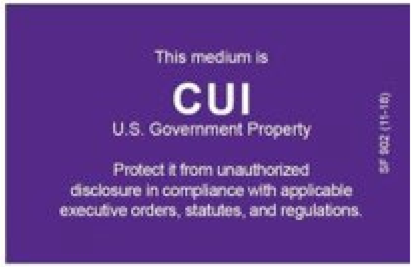
CMMC MODEL

Federal Contract Information (FCI)

- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems
- CMMC Level 1 Self-Assessment Guide

Controlled Unclassified Information (CUI)

- DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting
- NIST SP 800-171 / CMMC Level 2 Assessment Guide



This medium is

CUI

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

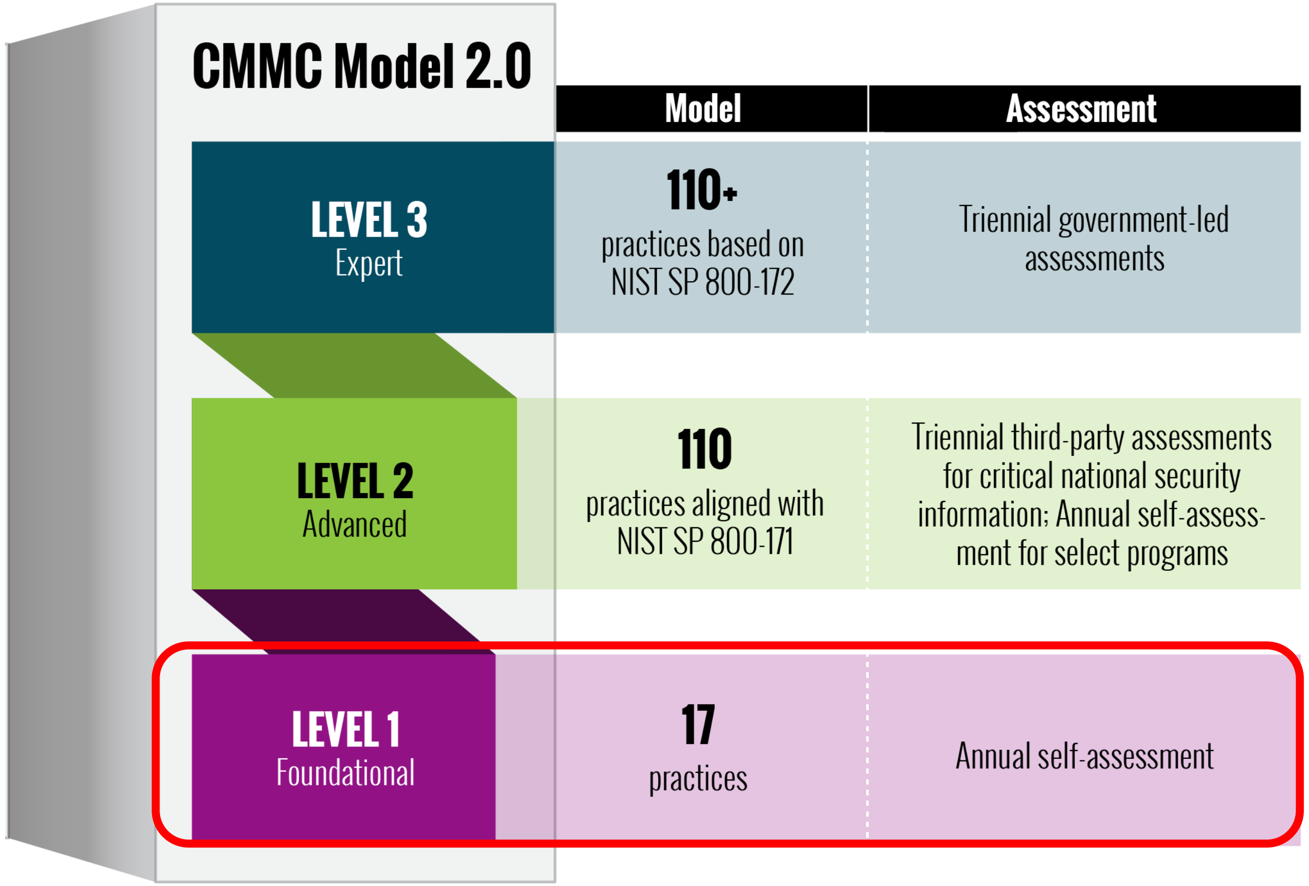
SF 902 (11-18)

Cybersec INVESTMENTS

PUBLIC

Public Release Authorized

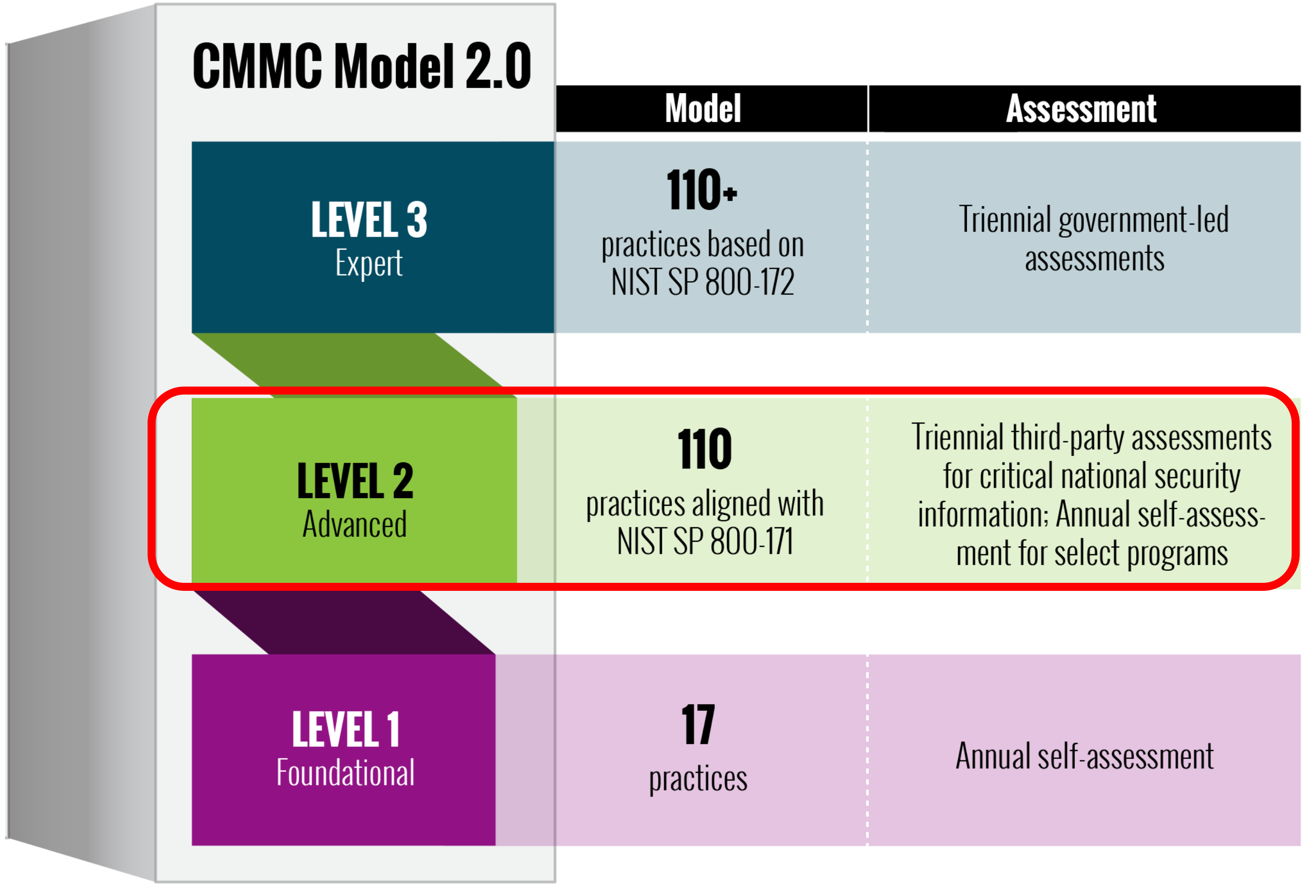
CMMC MODEL: ASSESSMENTS



CMMC Model 2.0

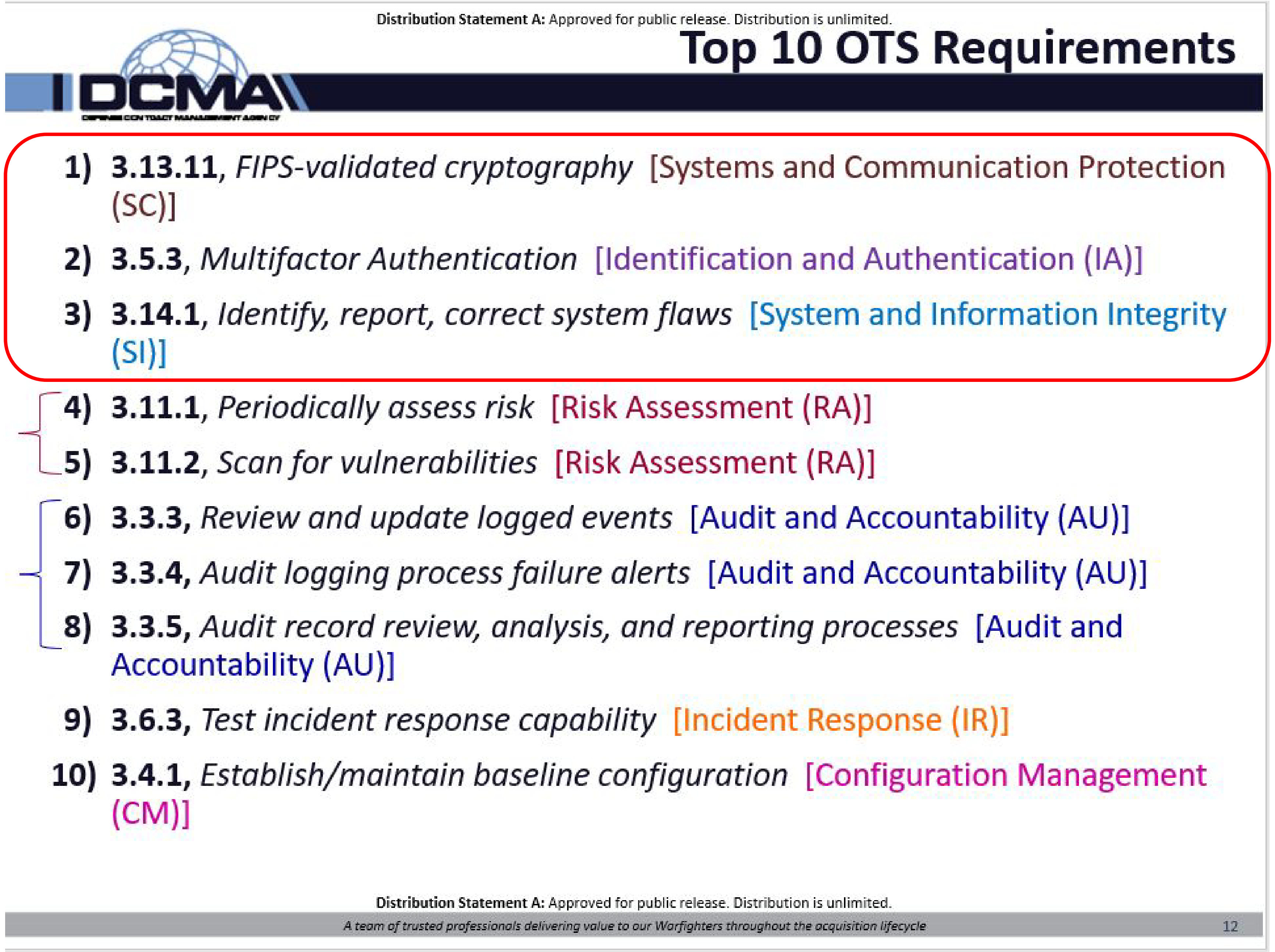
	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

CMMC MODEL: ASSESSMENTS



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment



Top 10 OTS Requirements

1) **3.13.11**, *FIPS-validated cryptography* [Systems and Communication Protection (SC)]
2) **3.5.3**, *Multifactor Authentication* [Identification and Authentication (IA)]
3) **3.14.1**, *Identify, report, correct system flaws* [System and Information Integrity (SI)]
4) **3.11.1**, *Periodically assess risk* [Risk Assessment (RA)]
5) **3.11.2**, *Scan for vulnerabilities* [Risk Assessment (RA)]
6) **3.3.3,** *Review and update logged events* [Audit and Accountability (AU)]
7) **3.3.4,** *Audit logging process failure alerts* [Audit and Accountability (AU)]
8) **3.3.5,** *Audit record review, analysis, and reporting processes* [Audit and Accountability (AU)]
9) **3.6.3,** *Test incident response capability* [Incident Response (IR)]
10) **3.4.1,** *Establish/maintain baseline configuration* [Configuration Management (CM)]

NIST SP 800-171 PARAGRAPH 1.1
PURPOSE AND APPLICABILITY

- The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING
CONTROLLED UNCLASSIFIED
INFORMATION IN NONFEDERAL
SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 PARAGRAPH 1.1
PURPOSE AND APPLICABILITY

- The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 PARAGRAPH 1.1
PURPOSE AND APPLICABILITY

- *System components include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.*

NIST SPECIAL PUBLICATION

SP 800-171

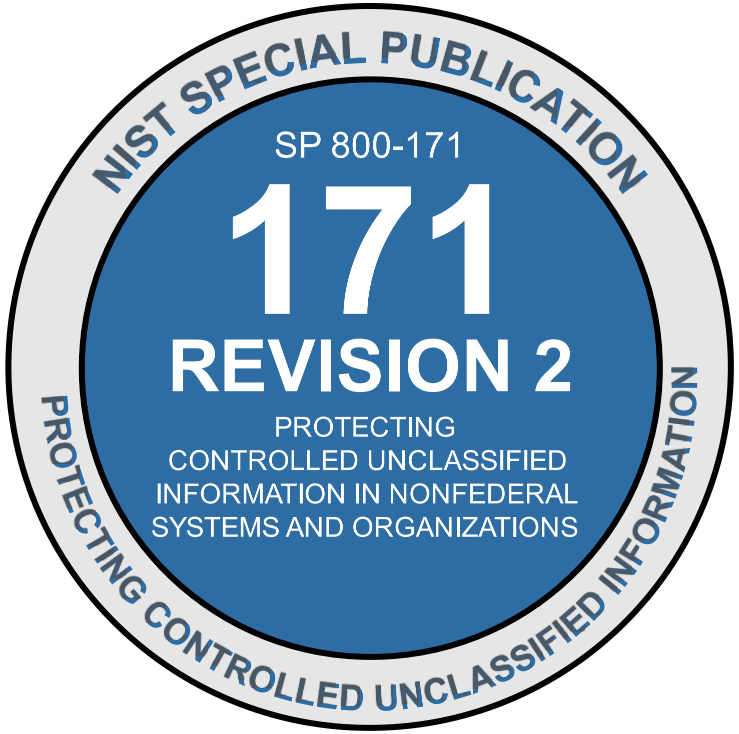
171

REVISION 2

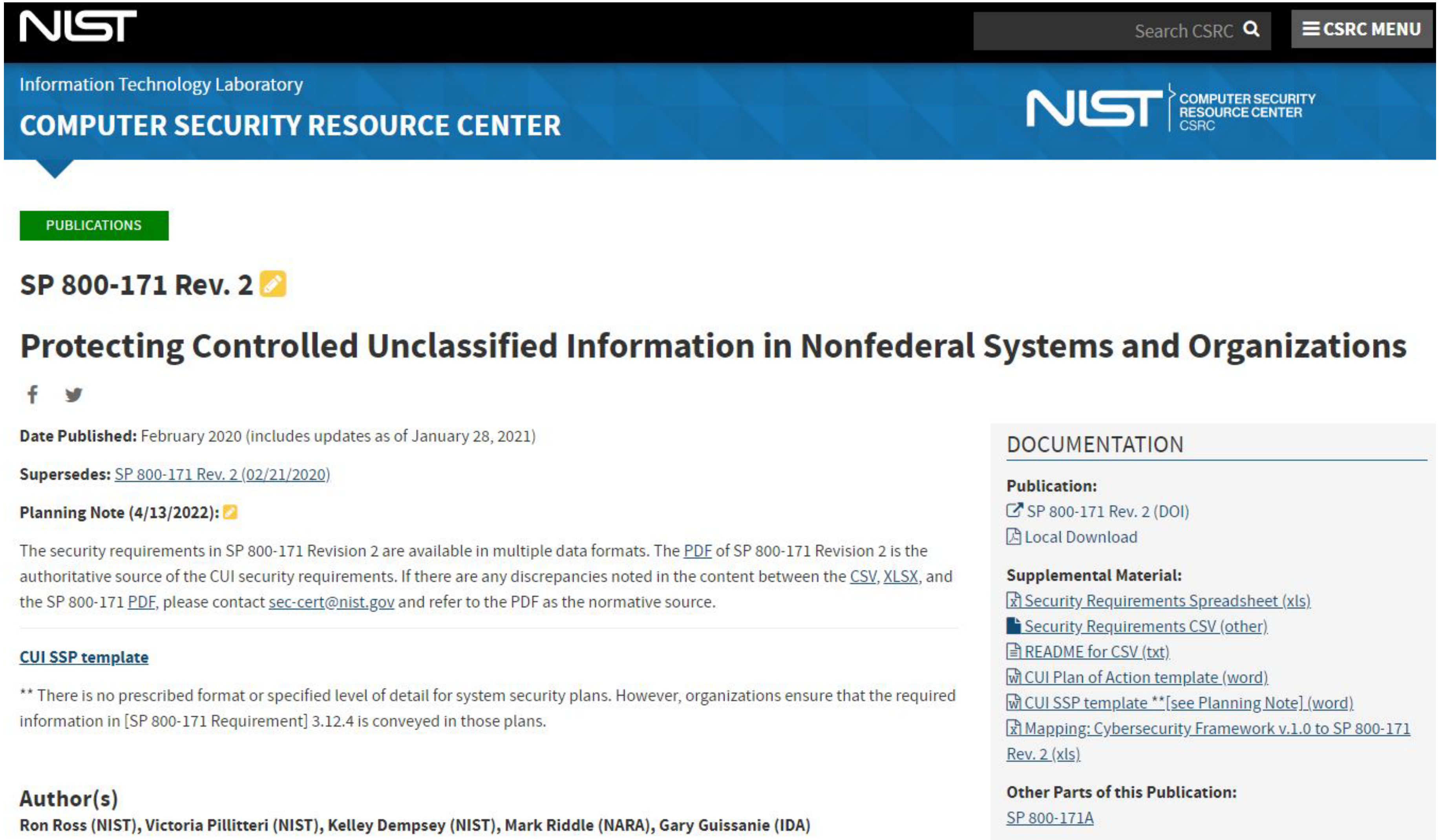
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 VERSUS NIST SP 800-171A


NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING
CONTROLLED UNCLASSIFIED
INFORMATION IN NONFEDERAL
SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SPECIAL PUBLICATION
SP 800-171A
171A
ASSESSING SECURITY
REQUIREMENTS FOR
CONTROLLED UNCLASSIFIED
INFORMATION
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION


NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
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 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), 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)

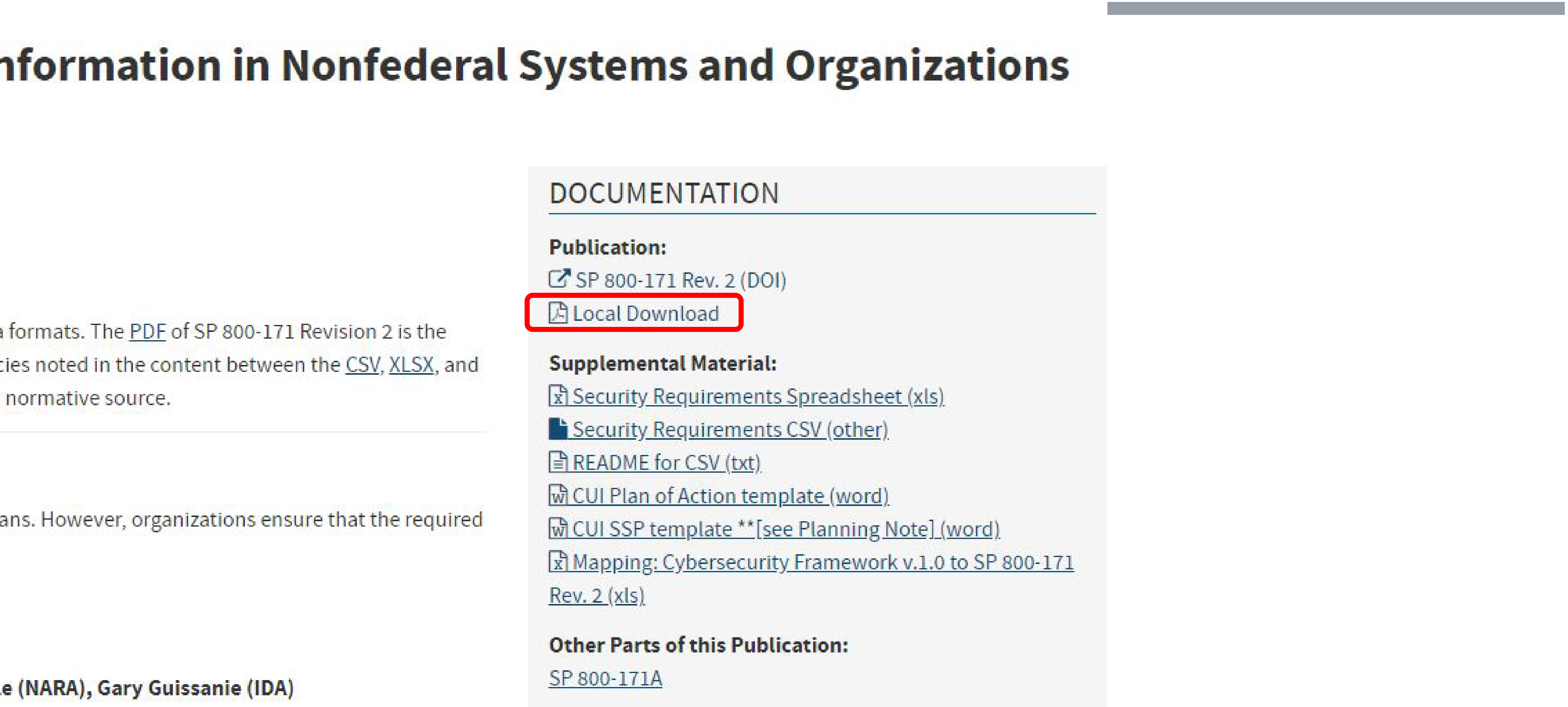
CUI Plan of Action template (word)

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



nformation in Nonfederal Systems and Organizations

a formats. The PDF of SP 800-171 Revision 2 is the
cies noted in the content between the CSV, XLSX, and
normative source.

ans. However, organizations ensure that the required

e (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

SP 800-171 Rev. 2 (DOI)
Local Download

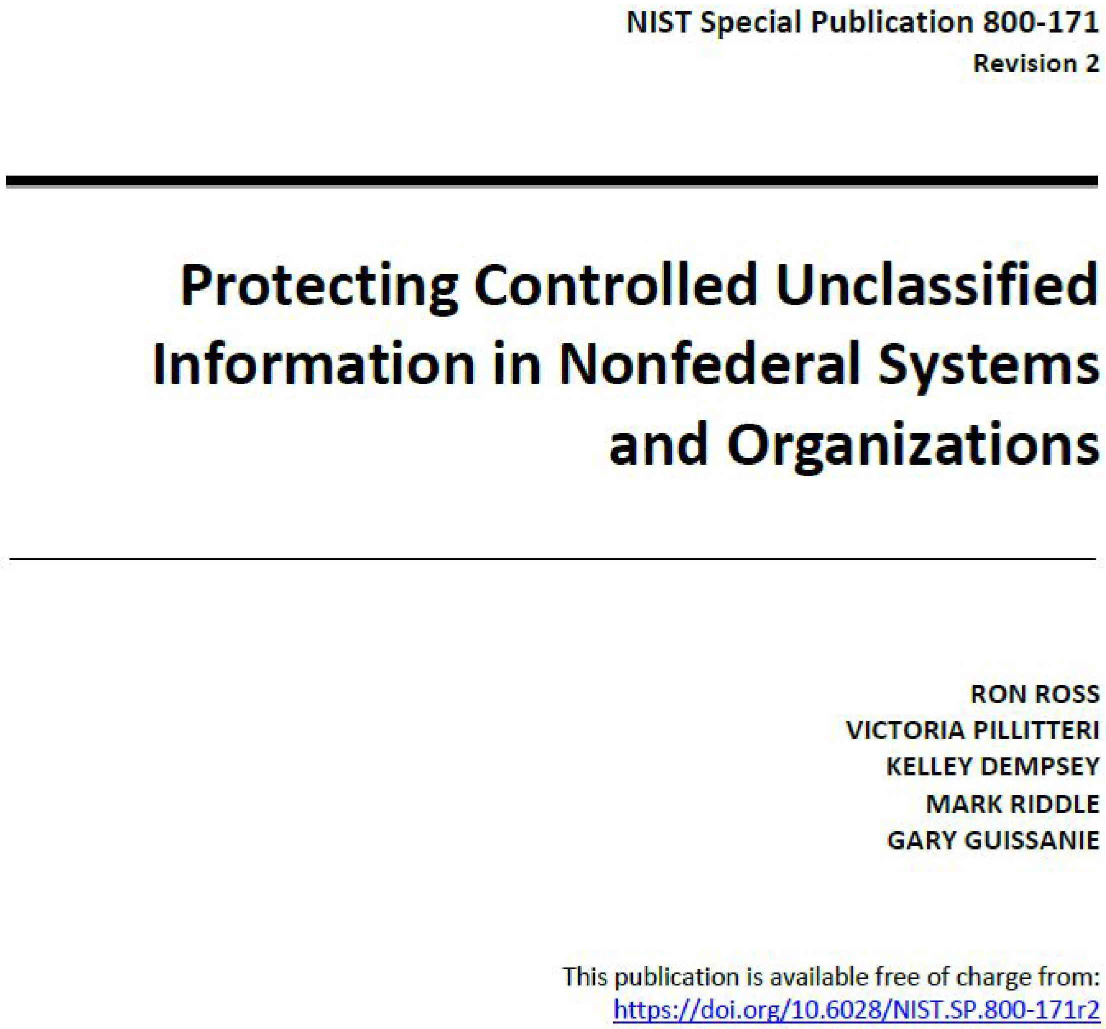
Supplemental Material:

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

NIST SP 800-171 VERSUS NIST SP 800-171A



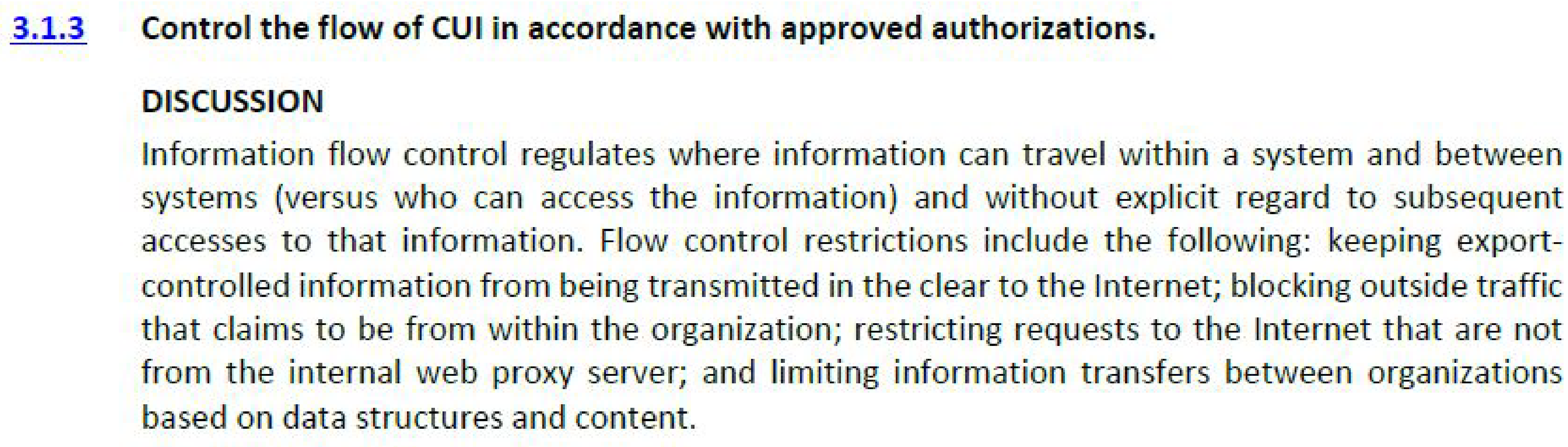
NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

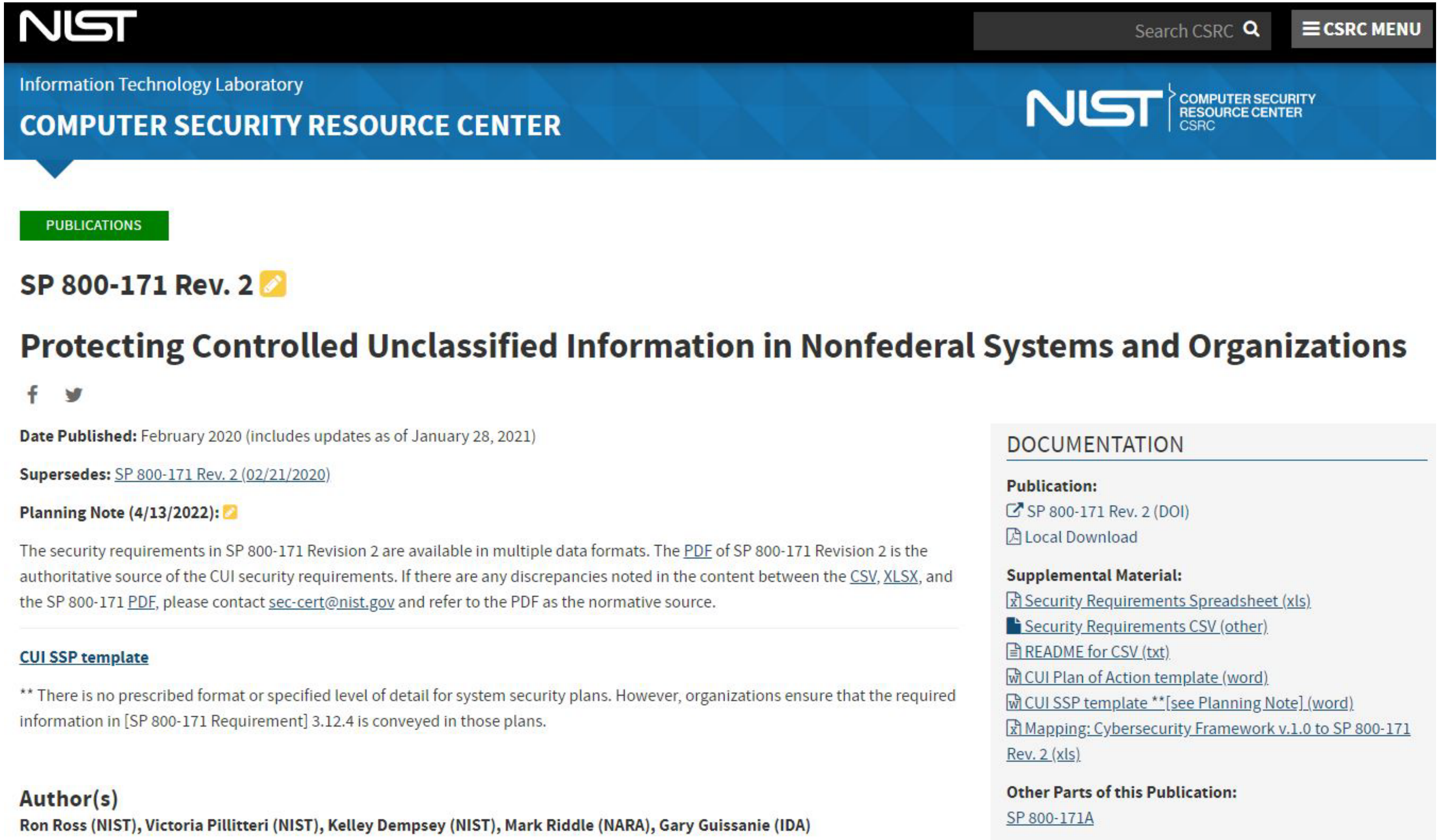
NIST SP 800-171 VERSUS NIST SP 800-171A



3.1.3 **Control the flow of CUI in accordance with approved authorizations.**

DISCUSSION

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

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

DOCUMENTATION

Publication:

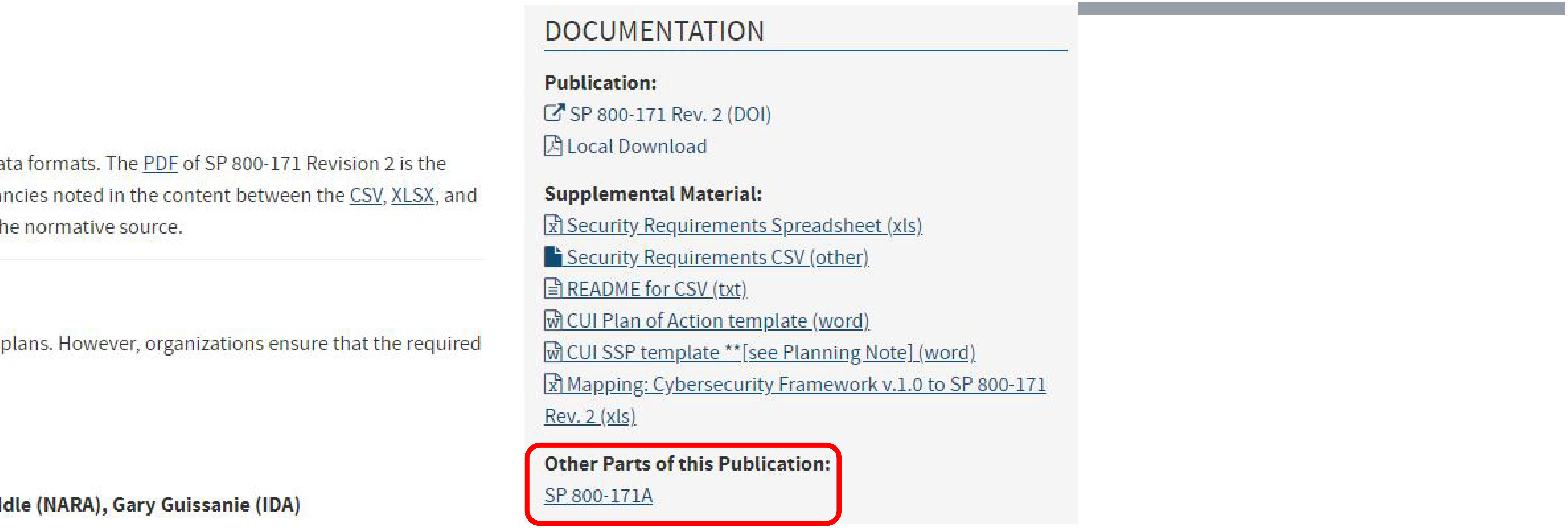
- SP 800-171 Rev. 2 (DOI)
- Local Download

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



ata formats. The PDF of SP 800-171 Revision 2 is the
ncies noted in the content between the CSV, XLSX, and
he normative source.

plans. However, organizations ensure that the required

dle (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)

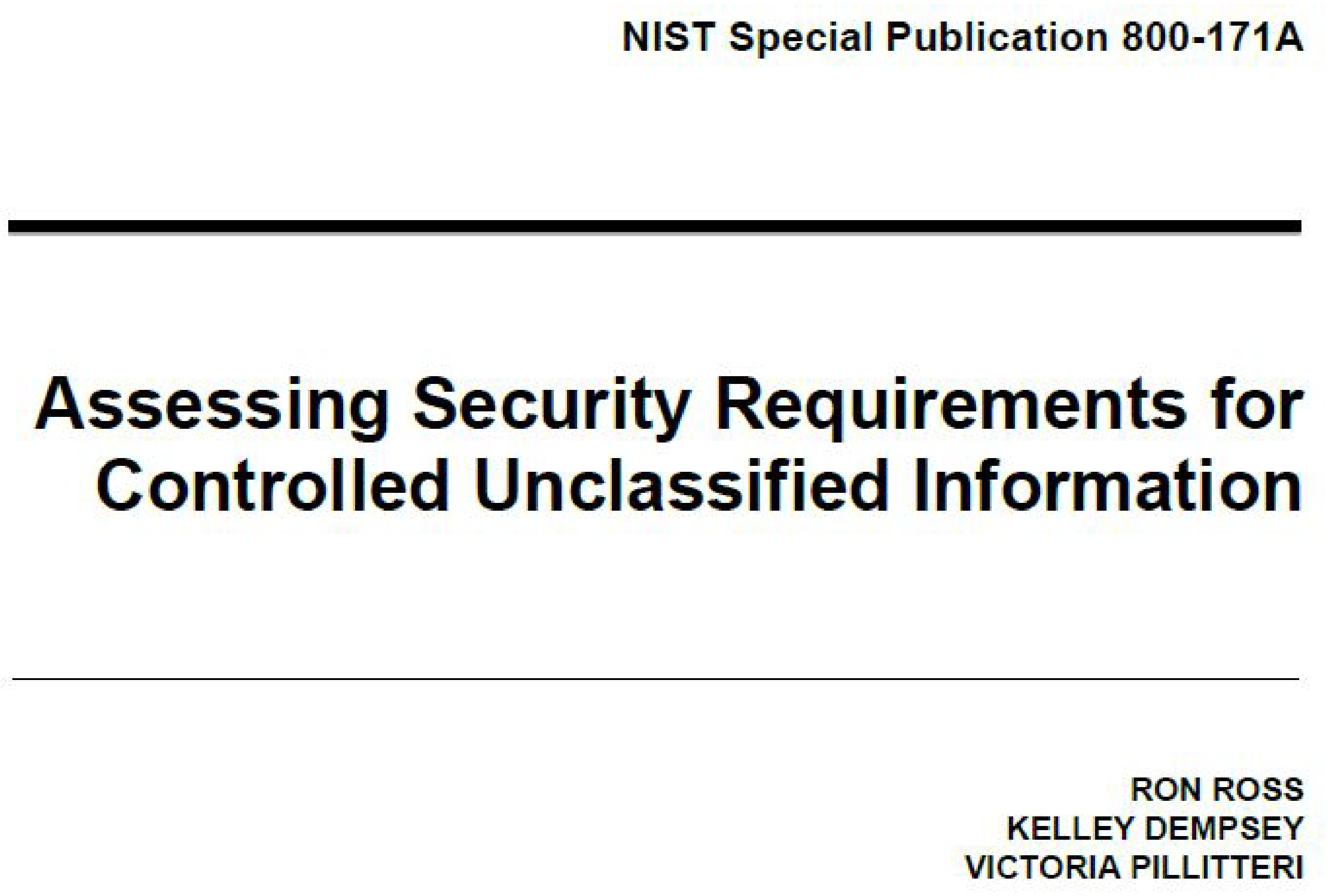
CUI SSP template **[see Planning Note] (word)

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

Other Parts of this Publication:

SP 800-171A

NIST SP 800-171 VERSUS NIST SP 800-171A

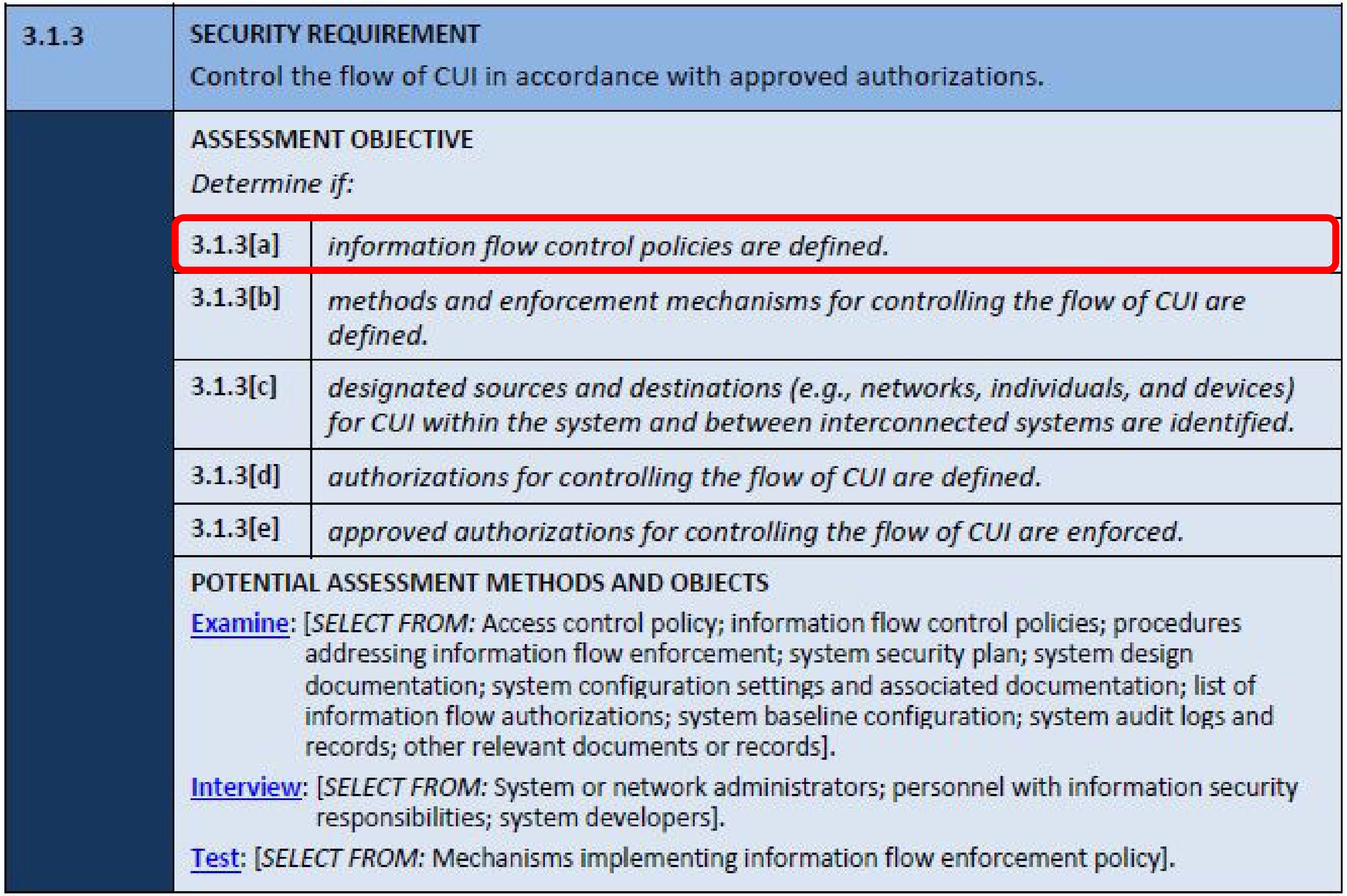


NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

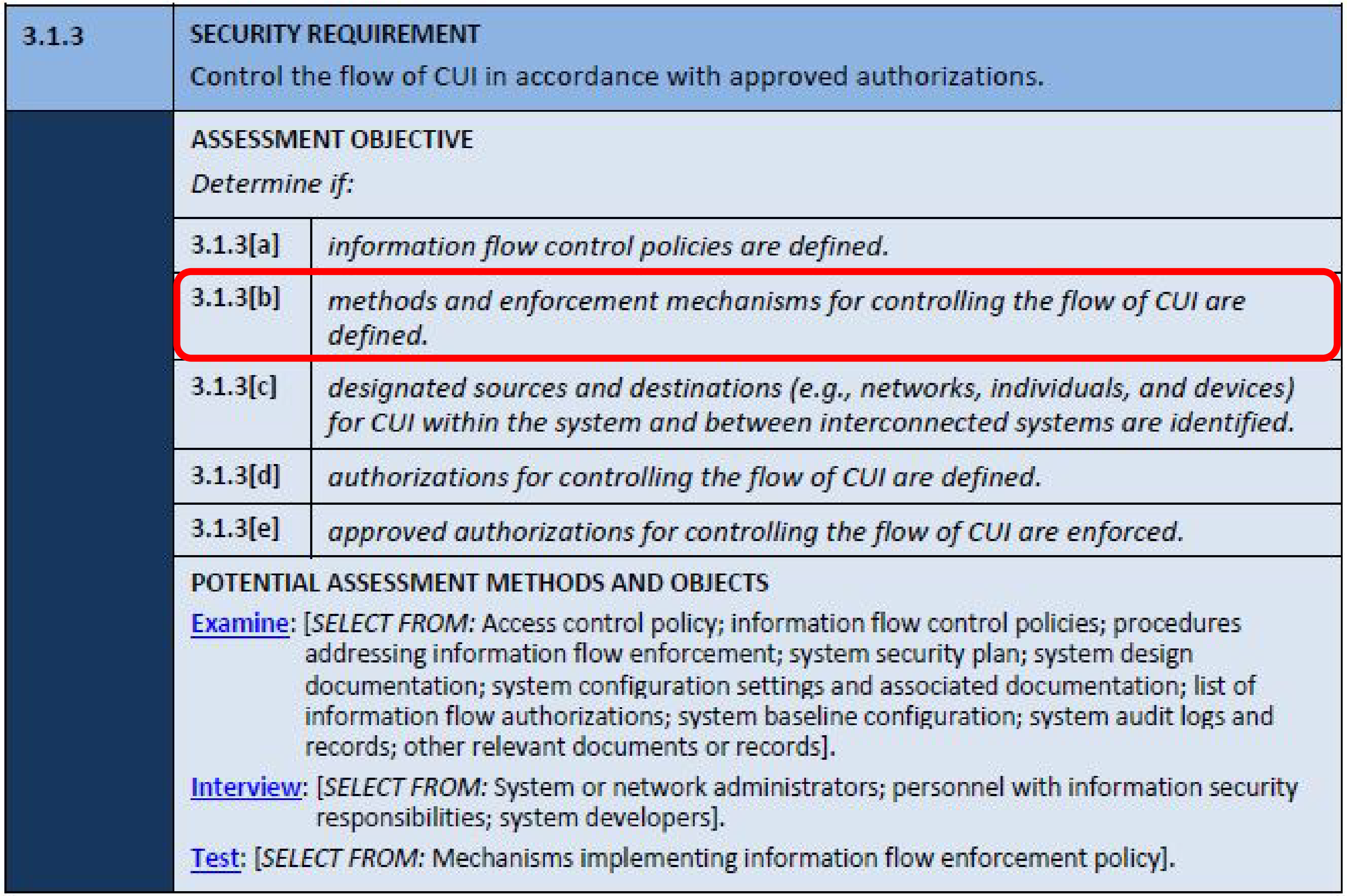
RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

NIST SP 800-171 VERSUS NIST SP 800-171A



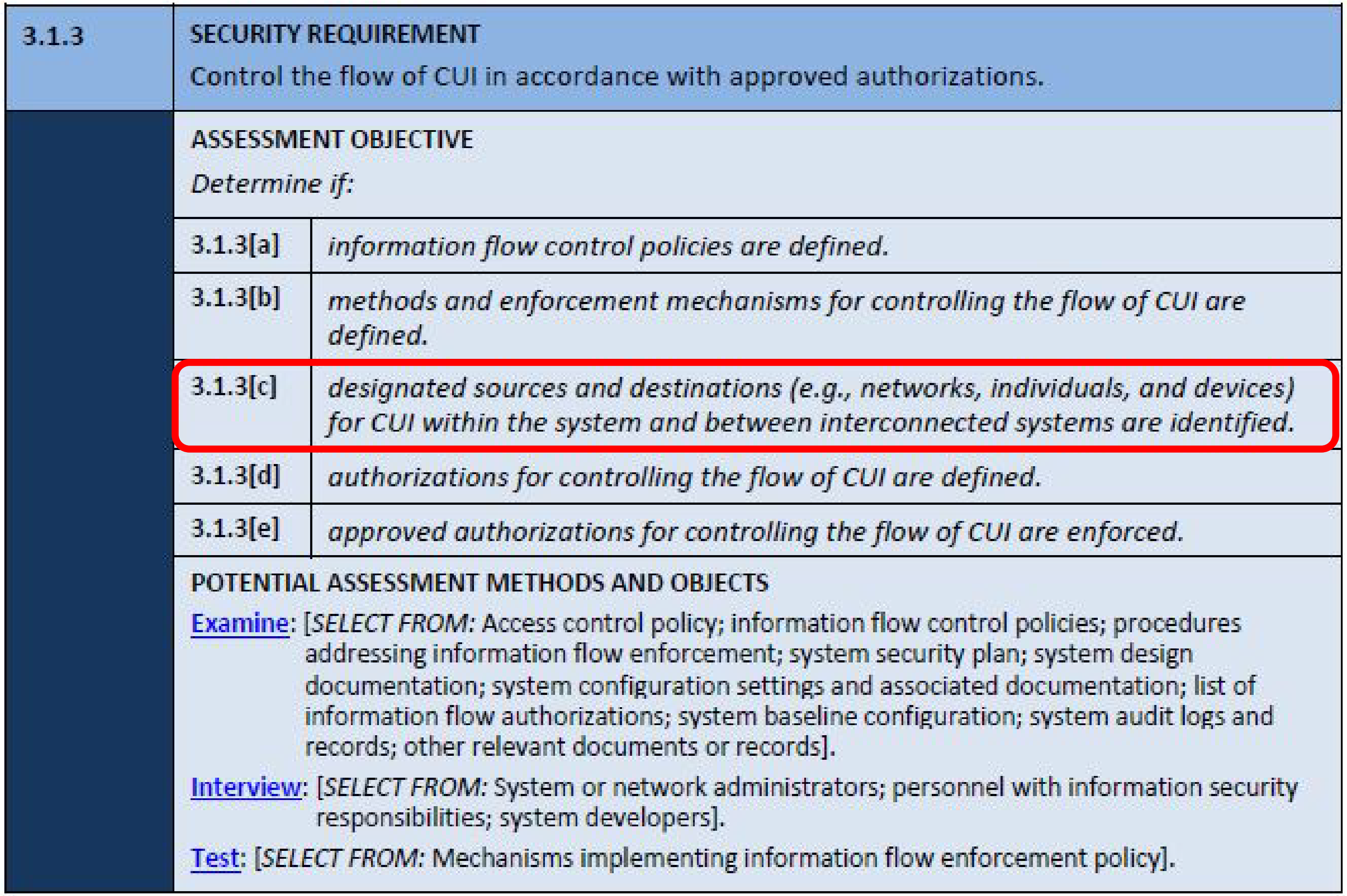
3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

NIST SP 800-171 VERSUS NIST SP 800-171A



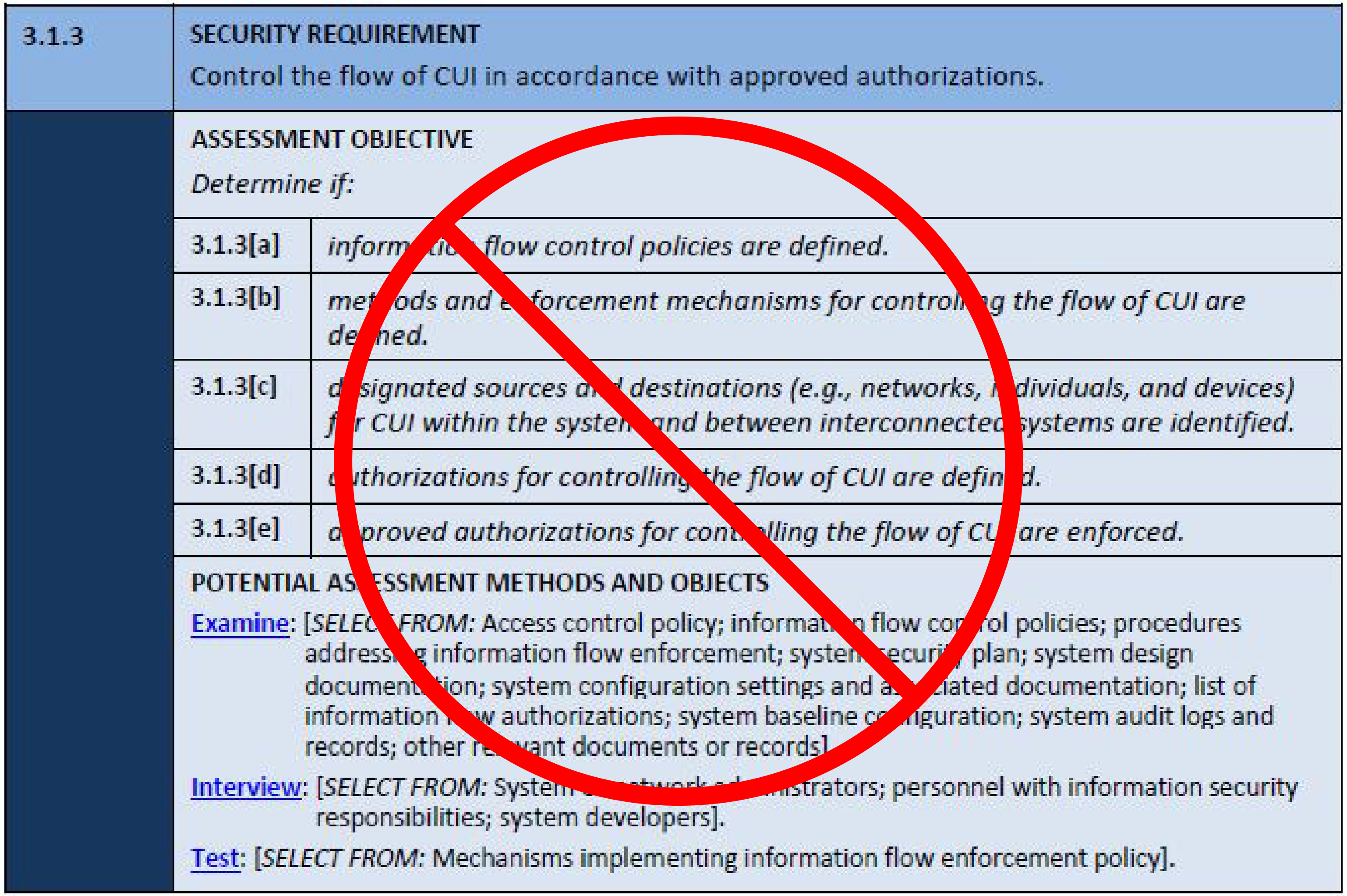
3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

NIST SP 800-171 VERSUS NIST SP 800-171A



3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
3.1.3[a]	*information flow control policies are defined.*
3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

NIST SP 800-171 VERSUS NIST SP 800-171A



3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

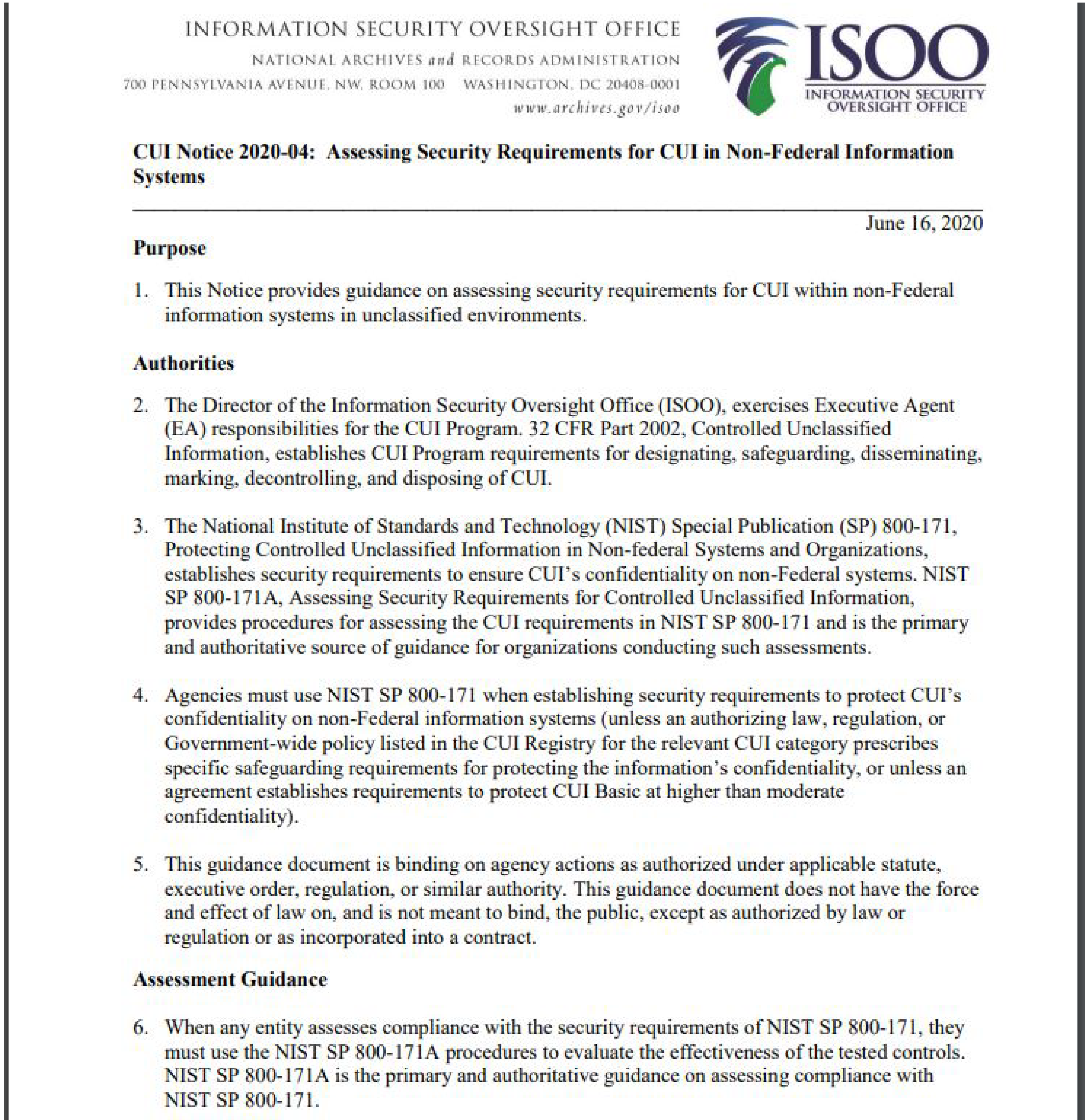
NIST SP 800-171 VERSUS NIST SP 800-171A

- 110 requirements

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

- 320 assessment objectives

NIST SPECIAL PUBLICATION
SP 800-171A
171A
ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION



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

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

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.

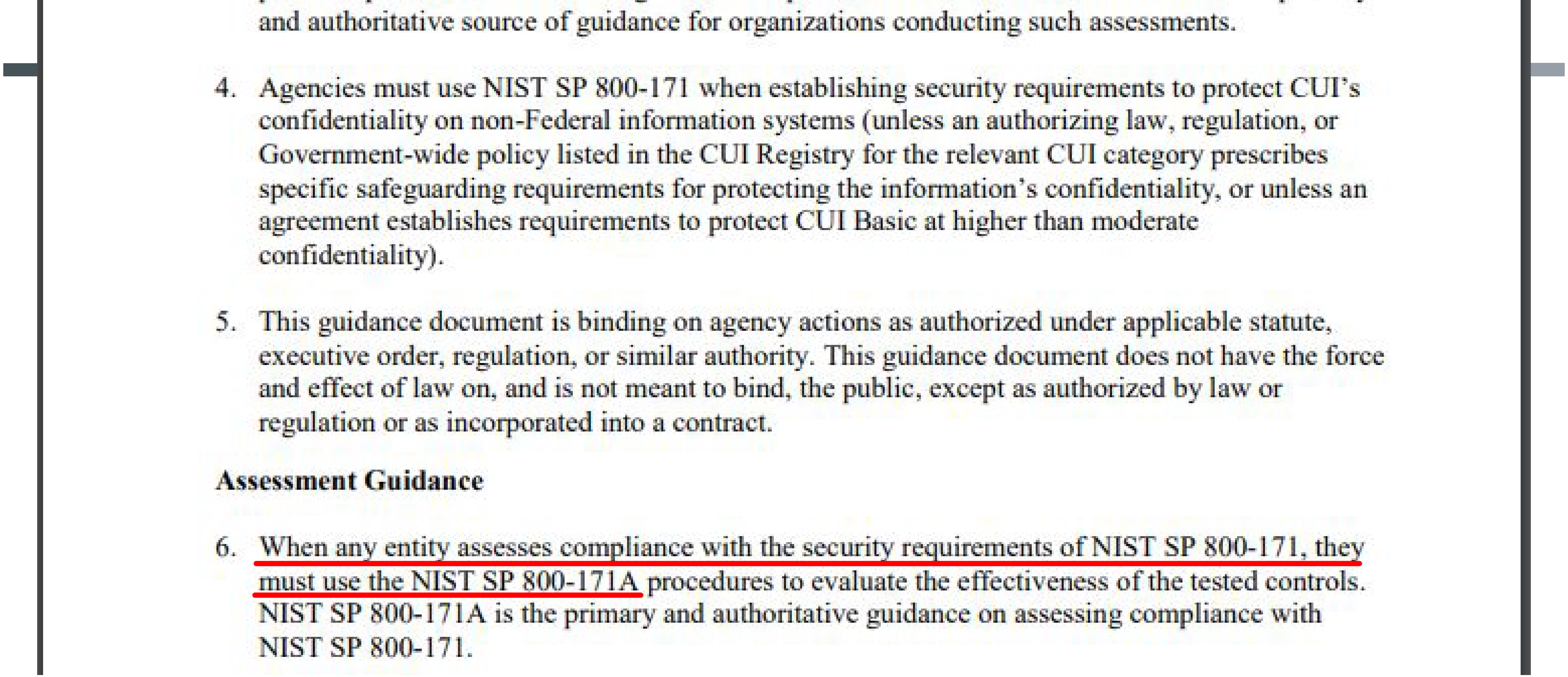
3. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, establishes security requirements to ensure CUI's confidentiality on non-Federal systems. NIST SP 800-171A, Assessing 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.



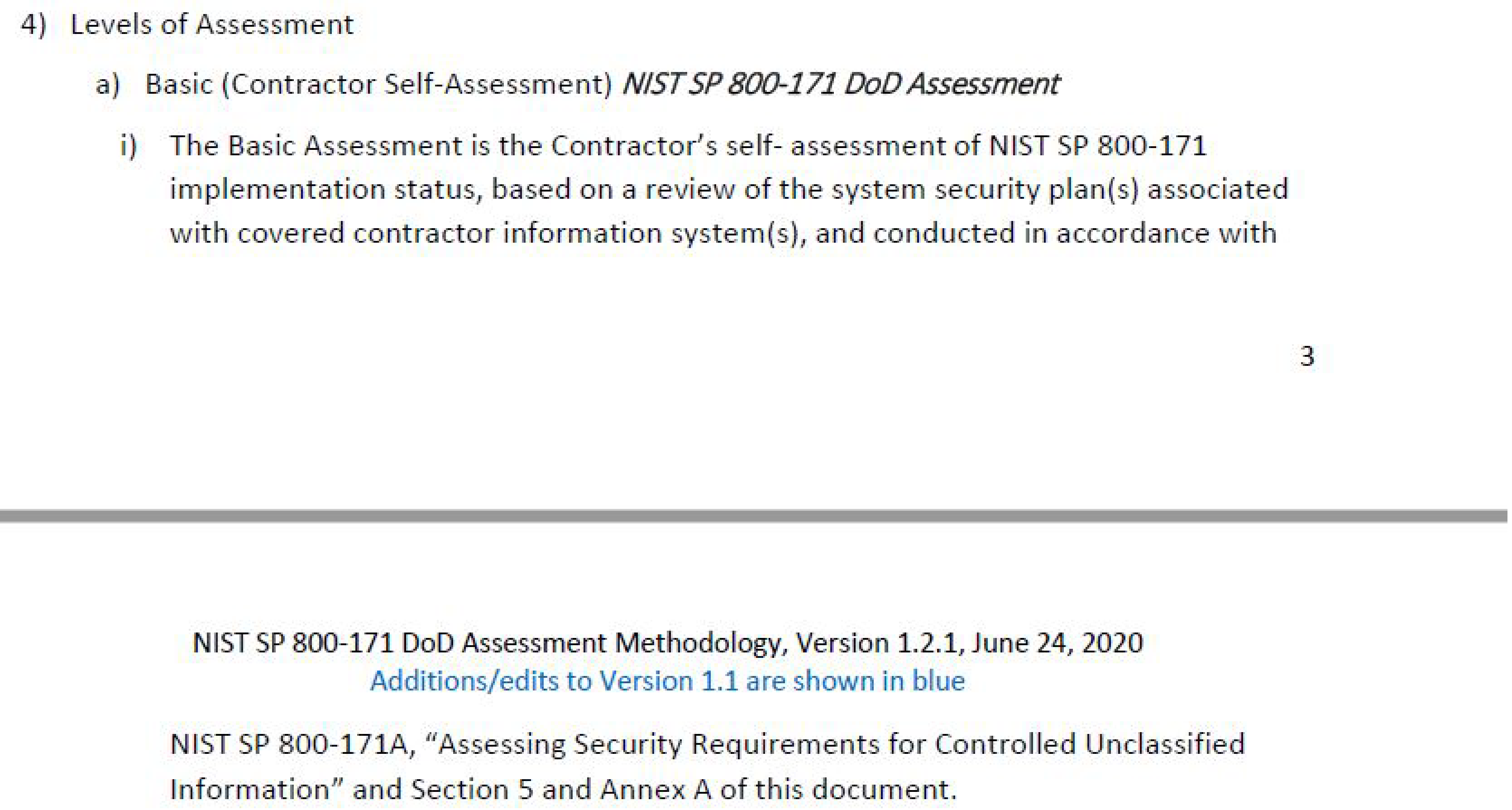
and authoritative source of guidance for organizations conducting such assessments.

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.

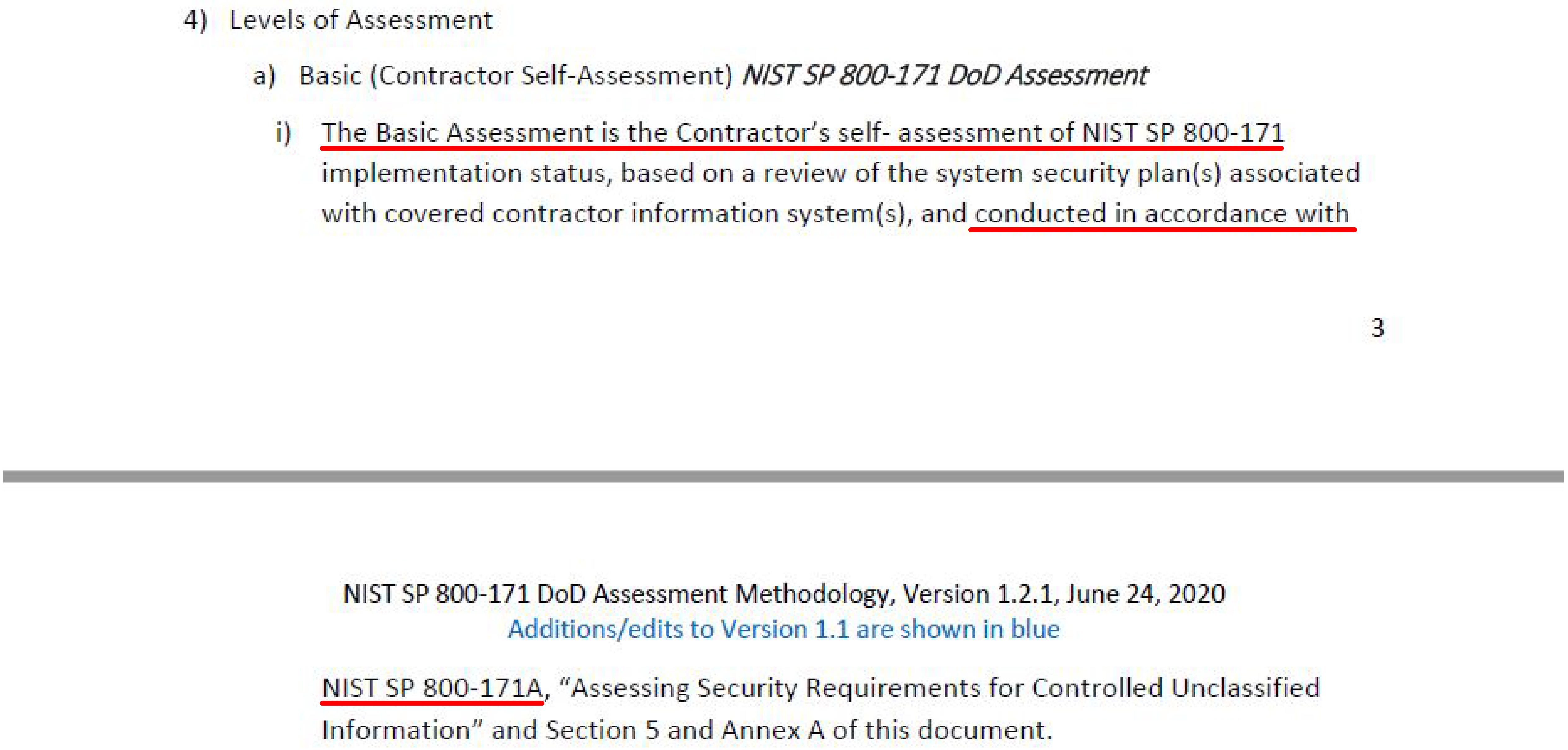


4) Levels of Assessment

a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.



4) Levels of Assessment

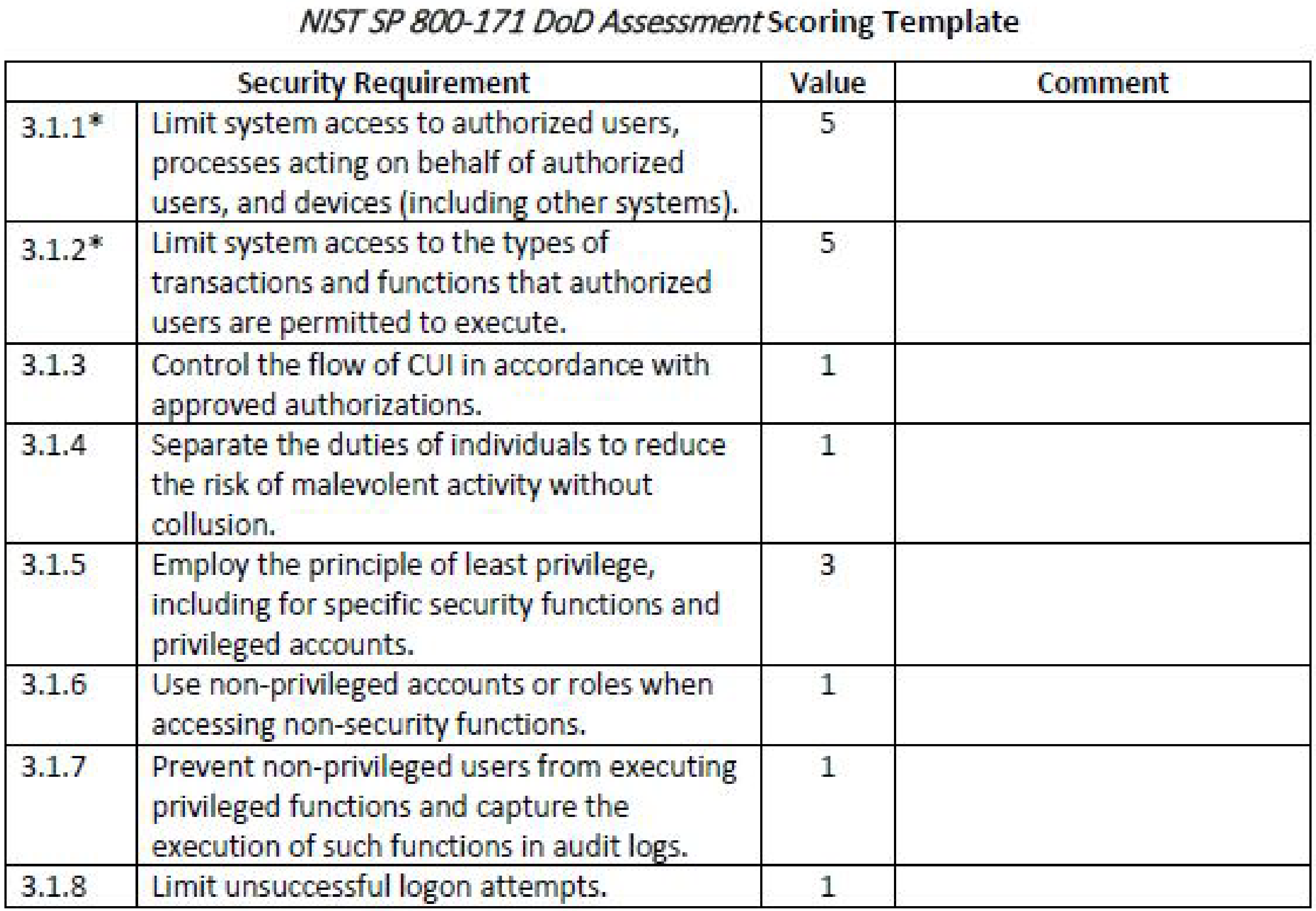
a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

3

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020
Additions/edits to Version 1.1 are shown in blue

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.

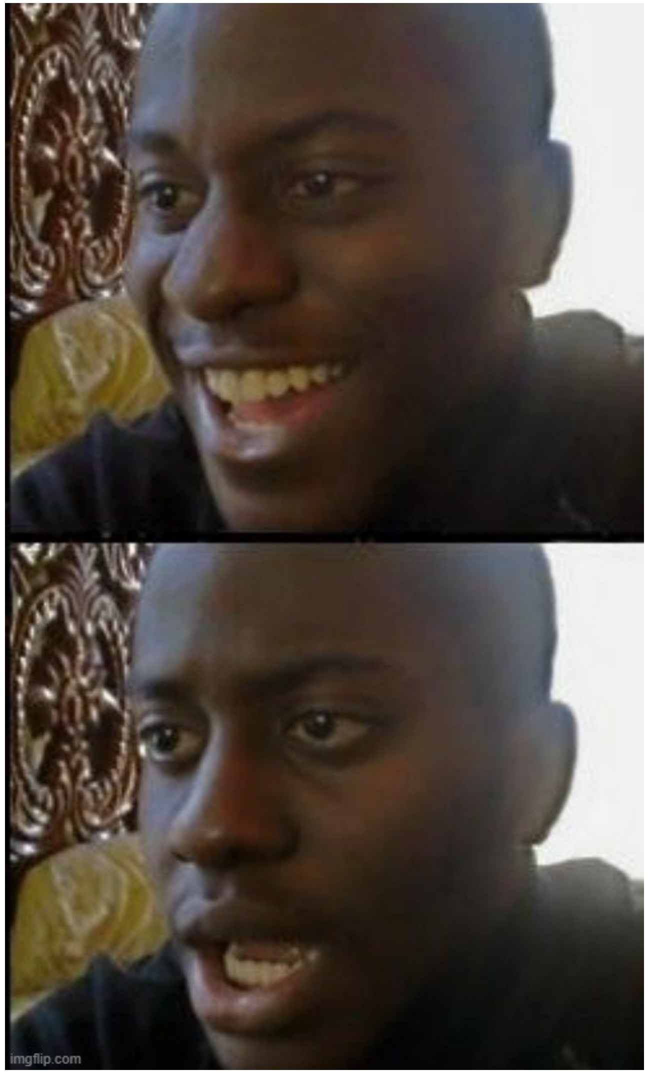


NIST SP 800-171 DoD Assessment Scoring Template

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

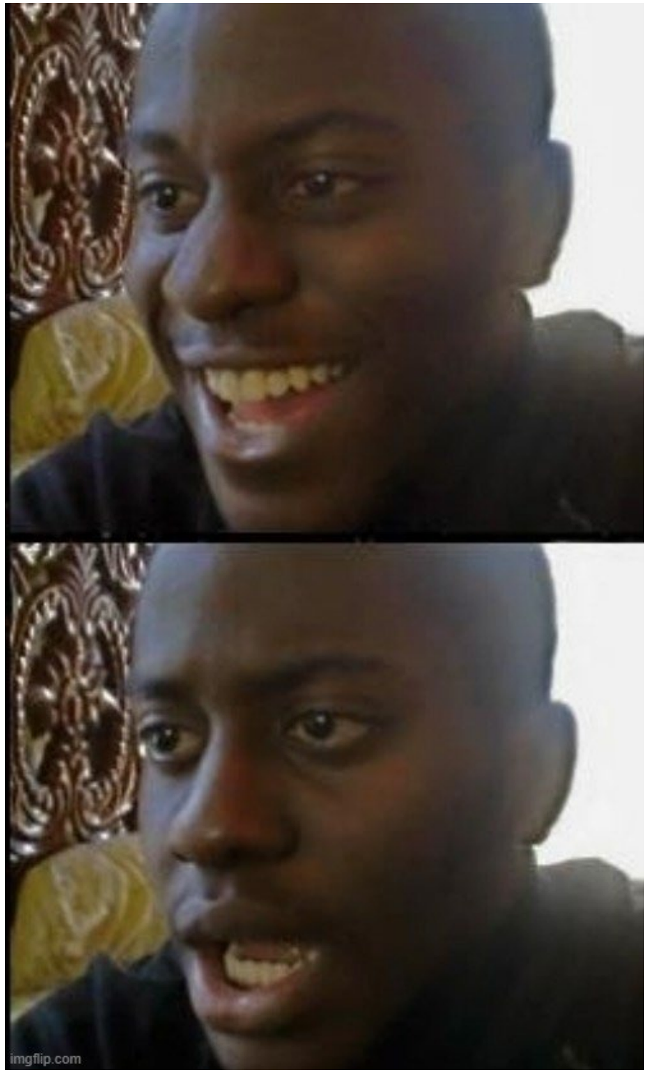
DOD ASSESSMENT METHODOLOGY V1.2.1

110



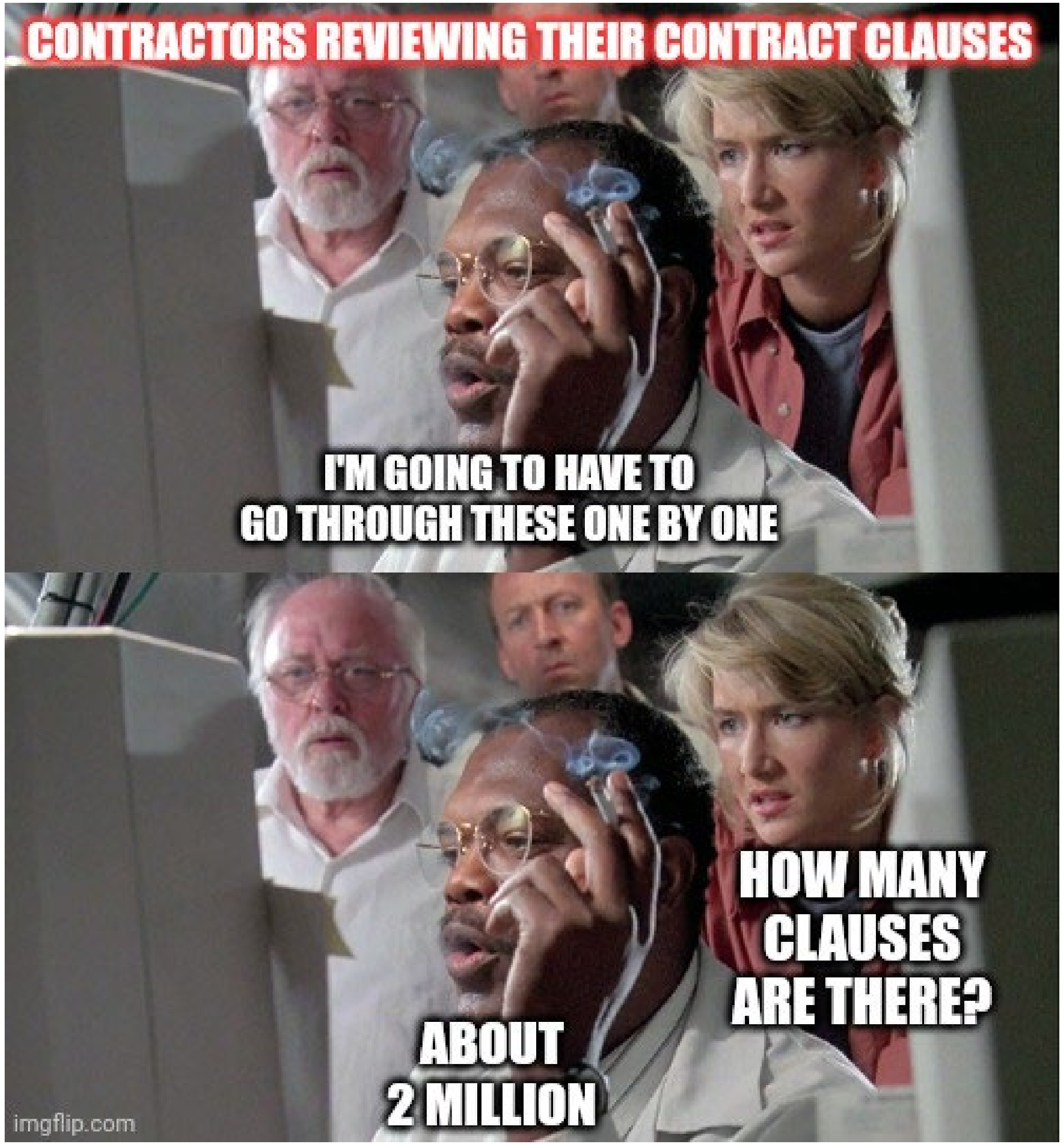
DOD ASSESSMENT METHODOLOGY V1.2.1

-203



DFARS 252.204-7012, DFARS 252.204-7019, AND DFARS 252.204-7020

DFARS 252.204-7012


CONTRACTORS REVIEWING THEIR CONTRACT CLAUSES
I'M GOING TO HAVE TO GO THROUGH THESE ONE BY ONE
HOW MANY CLAUSES ARE THERE?
ABOUT 2 MILLION
imgflip.com

DFARS 252.204-7012(B)(2)(II)(D)

- *(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

FedRAMP

Cybersec INVESTMENTS

PUBLIC
Public Release Authorized

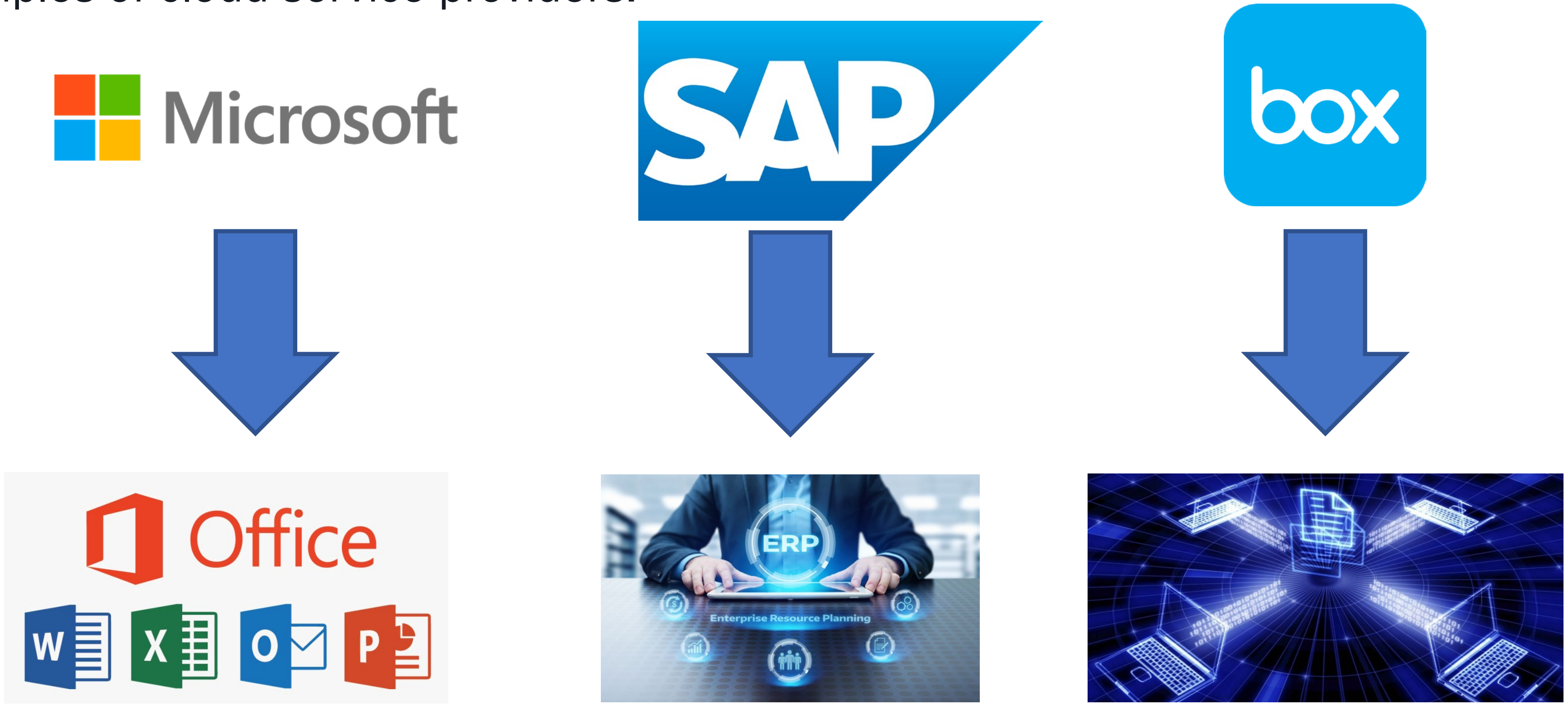
DFARS 252.204-7012(B)(2)(II)(D)

- *(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

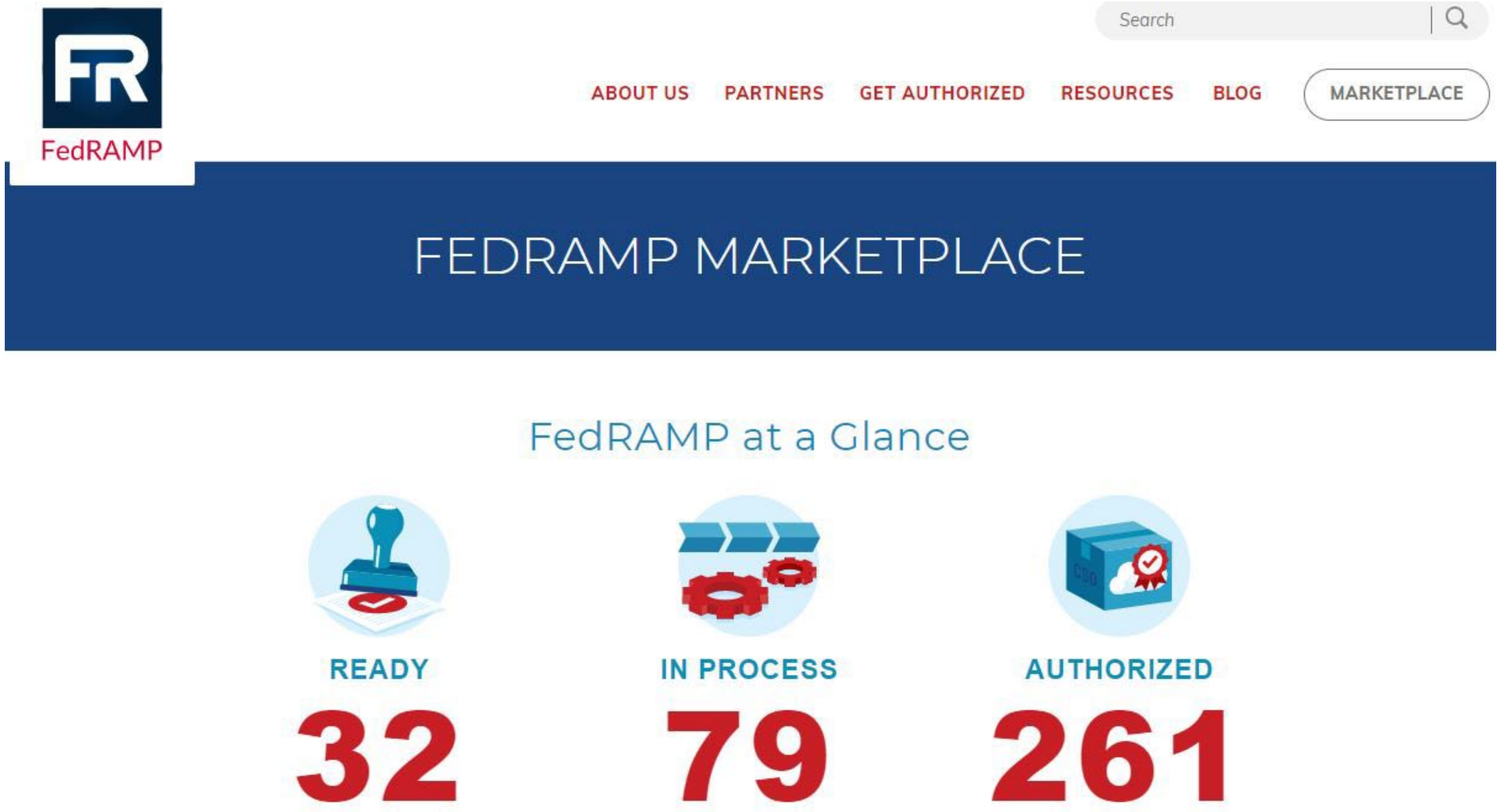
FedRAMP

DFARS 252.204-7012(B)(2)(II)(D)

- Examples of cloud service providers:



FEDRAMP MARKETPLACE

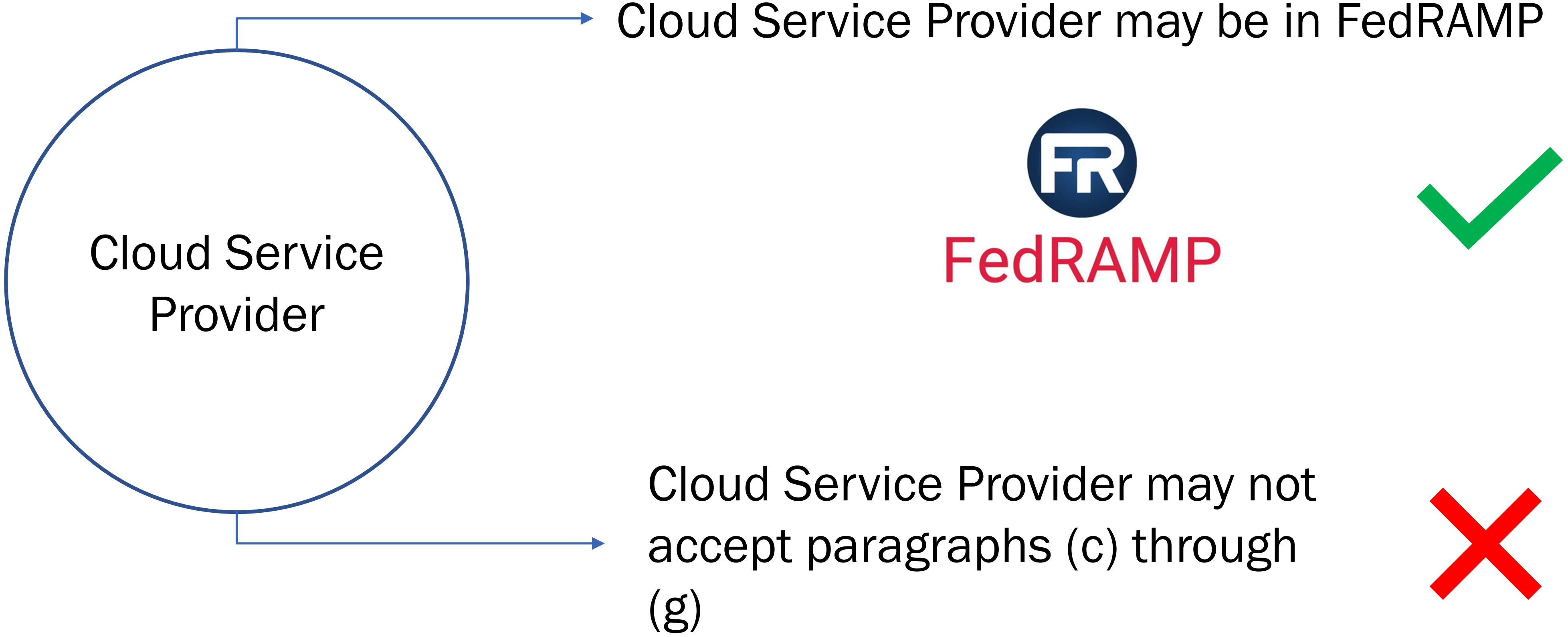


FEDRAMP MARKETPLACE

FedRAMP at a Glance

READY	IN PROCESS	AUTHORIZED
32	79	261

DFARS 252.204-7012 REQUIREMENTS



Cloud Service Provider

Cloud Service Provider may be in FedRAMP

FedRAMP ✓

Cloud Service Provider may not accept paragraphs (c) through (g) ✗

DFARS 252.204-7012 REQUIREMENTS

	Microsoft 365 "Commercial"			
Customer Eligibility	**Any customer**			
Datacenter Locations	**US & OCONUS**			
FedRAMP [1]	**High**			
DFARS 252.204-7012	**No**			
FCI + CMMC L1	**Yes**			
CUI / CDI + CMMC L2-3	**No**			
ITAR / EAR	**No**			
DoD CC SRG Level [2]	**N/A**			
NIST SP 800-53 / 171 [3]	**Yes**			
CJIS Agreement	**No**			
NERC / FERC	**No**			
Customer Support	Worldwide / Commercial Personnel			
Directory / Network	Azure "Commercial"			

[1] *Equivalency*, Supports accreditation at noted impact level
[2] *Equivalency*, PA issued for DoD only
[3] Organizational Defined Values (ODV's) will vary
^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

DFARS 252.204-7012 REQUIREMENTS

	Microsoft 365 “Commercial”			
Customer Eligibility	**Any customer**			
Datacenter Locations	**US & OCONUS**			
FedRAMP [1]	**High**			
DFARS 252.204-7012	**No**			
FCI + CMMC L1	**Yes**			
CUI / CDI + CMMC L2-3	**No**			
ITAR / EAR	**No**			
DoD CC SRG Level [2]	**N/A**			
NIST SP 800-53 / 171 [3]	**Yes**			
CJIS Agreement	**No**			
NERC / FERC	**No**			
Customer Support	Worldwide / Commercial Personnel			
Directory / Network	Azure “Commercial”			

[1] *Equivalency*, Supports accreditation at noted impact level
[2] *Equivalency*, PA issued for DoD only
[3] Organizational Defined Values (ODV’s) will vary
^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

DFARS 252.204-7019 REQUIREMENTS

DFARS 252.204-7019 REQUIREMENTS

- *(b) Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171.*

DFARS 252.204-7019 REQUIREMENTS

- *(b) Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171.*

DFARS 252.204-7020 REQUIREMENTS

DFARS 252.204-7020 REQUIREMENTS

- *(c) Requirement. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, if necessary.*

DFARS 252.204-7020 REQUIREMENTS

- *(c) Requirement. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, if necessary.*

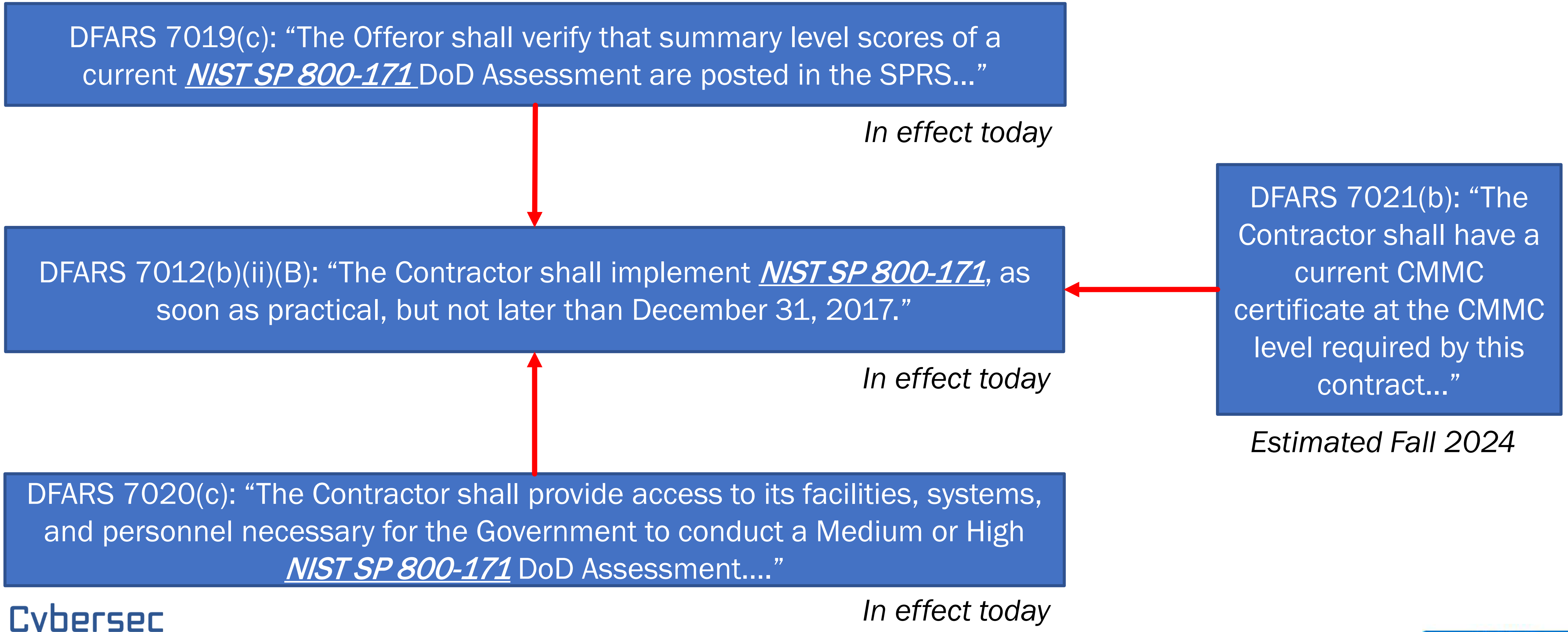
DFARS 252.204-7020 REQUIREMENTS

- ***(g) Subcontracts.*** *The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171 , for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government*

DFARS 252.204-7020 REQUIREMENTS

- *(g) Subcontracts. The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171 , for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government*

CMMC ASSESSES *EXISTING* REQUIREMENTS IN DFARS 7012



DFARS 7019(c): “The Offeror shall verify that summary level scores of a current *NIST SP 800-171* DoD Assessment are posted in the SPRS…”

In effect today

DFARS 7012(b)(ii)(B): “The Contractor shall implement *NIST SP 800-171*, as soon as practical, but not later than December 31, 2017.”

In effect today

DFARS 7021(b): “The Contractor shall have a current CMMC certificate at the CMMC level required by this contract…”

Estimated Fall 2024

DFARS 7020(c): “The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High *NIST SP 800-171* DoD Assessment….”

In effect today

$ 500

What is the primary and authoritative guidance on assessing compliance with NIST SP 800-171?

A: NIST SP 800-171

B: NIST SP 800-53

C: NIST SP 800-171A

D NIST SP 800-53A
:

$ 500

What is the primary and authoritative guidance on assessing compliance with NIST SP 800-171?

A: NIST SP 800-171

B: NIST SP 800-53

[✓ C: NIST SP 800-171A]

D NIST SP 800-53A

:

14	$ 1 MILLION
13	$ 500,000
12	$ 250,000
11	$ 100,000
10	$ 50,000
9	$ 30,000
8	$ 20,000
7	$ 10,000
6	$ 7,000
5	$ 5,000
4	$ 3,000
3	$ 2,000
2	$ 1,000
1 ◆	$ 500

$ 1000

How many requirements are in NIST SP 800-171A?

A: 320

B: 432

C: 110

D: Too damn many

WHO WANTS TO BE A MILLIONAIRE SPECIAL EDITIONS WHO WANTS TO BE A

$ 1000

How many requirements are in NIST SP 800-171A?

[✓ A: 320]

B: 432

C: 110

D: Too damn many

14		$ 1 MILLION
13		$ 500,000
12		$ 250,000
11		$ 100,000
10		$ 50,000
9		$ 30,000
8		$ 20,000
7		$ 10,000
6		$ 7,000
5		$ 5,000
4		$ 3,000
3		$ 2,000
2	◆	$ 1,000
1	◆	$ 500

WHO WANTS TO BE A MILLIONAIRE SPECIAL EDITIONS WHO WANTS TO BE A

$ 2000

What is the lowest possible score according to the NIST SP 800-171 DoD Assessment Scoring Template?

A: 0

B: -203

C: -110

D 171
:

$ 2000

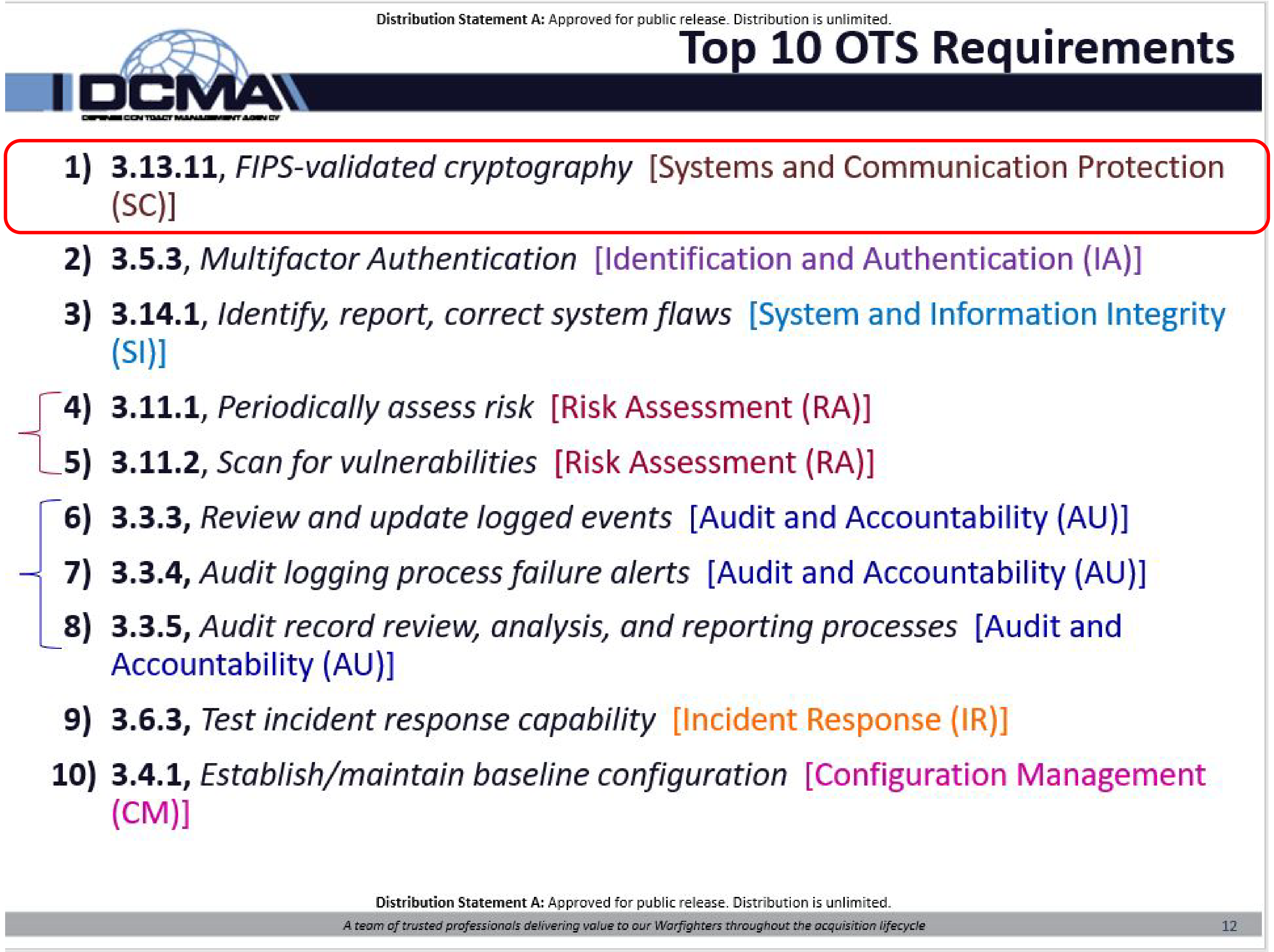
What is the lowest possible score according to the NIST SP 800-171 DoD Assessment Scoring Template?

A: 0

[✓ B: -203]

C: -110

D: 171



Distribution Statement A: Approved for public release. Distribution is unlimited.

Top 10 OTS Requirements

1) **3.13.11**, *FIPS-validated cryptography* [Systems and Communication Protection (SC)]
2) **3.5.3**, *Multifactor Authentication* [Identification and Authentication (IA)]
3) **3.14.1**, *Identify, report, correct system flaws* [System and Information Integrity (SI)]
4) **3.11.1**, *Periodically assess risk* [Risk Assessment (RA)]
5) **3.11.2**, *Scan for vulnerabilities* [Risk Assessment (RA)]
6) **3.3.3,** *Review and update logged events* [Audit and Accountability (AU)]
7) **3.3.4,** *Audit logging process failure alerts* [Audit and Accountability (AU)]
8) **3.3.5,** *Audit record review, analysis, and reporting processes* [Audit and Accountability (AU)]
9) **3.6.3,** *Test incident response capability* [Incident Response (IR)]
10) **3.4.1,** *Establish/maintain baseline configuration* [Configuration Management (CM)]

Distribution Statement A: Approved for public release. Distribution is unlimited.

A team of trusted professionals delivering value to our Warfighters throughout the acquisition lifecycle

PUBLIC
Public Release Authorized

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI

- *Determine if:*
  - *[a] FIPS-validated cryptography is employed to protect the confidentiality of CUI*

[A] FIPS-VALIDATED CRYPTOGRAPHY IS EMPLOYED TO PROTECT THE CONFIDENTIALITY OF CUI

- *Discussion*: *Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography.*

[A] FIPS-VALIDATED CRYPTOGRAPHY IS EMPLOYED TO PROTECT THE CONFIDENTIALITY OF CUI

- *<u>Discussion</u>: Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography.*

DOD PROCUREMENT TOOLBOX

- *Q72: Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11 – Do all of the 171 security requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?*

DOD PROCUREMENT TOOLBOX

- *A72: Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and http://csrc.nist.gov/groups/STM/cmvp/validation.html.*

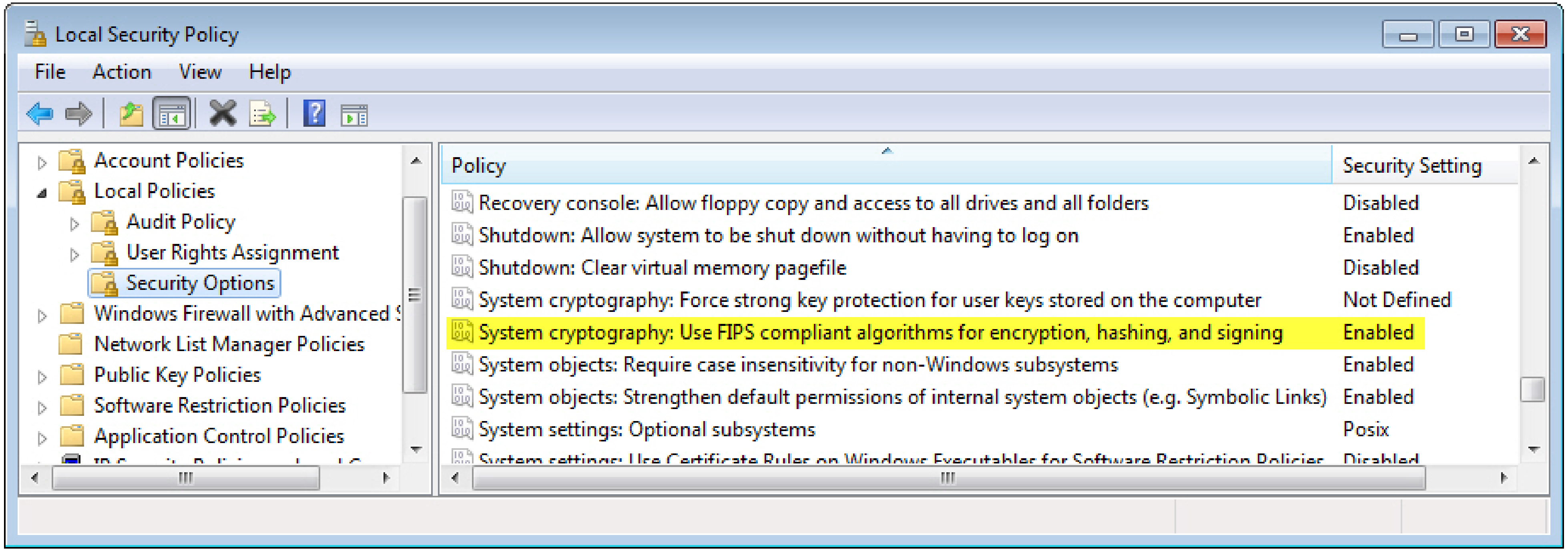
DOD PROCUREMENT TOOLBOX

- *A72: Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and http://csrc.nist.gov/groups/STM/cmvp/validation.html.*

DOD PROCUREMENT TOOLBOX (CONTINUED)

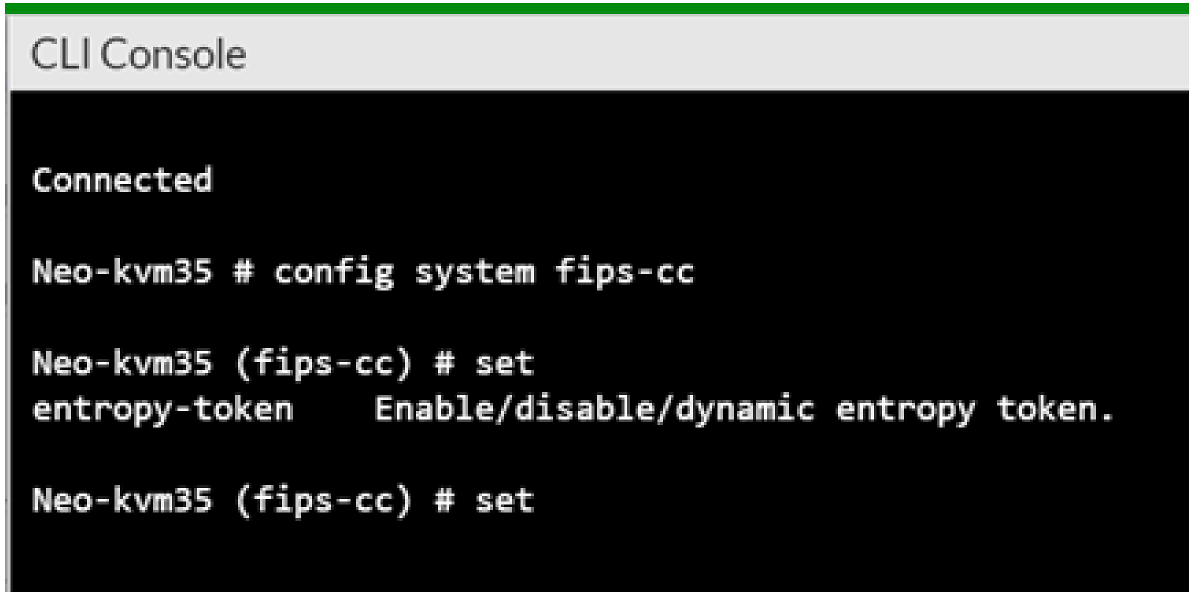
- *A72: When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI (or in this case covered defense information). Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system).*

[A] FIPS-VALIDATED CRYPTOGRAPHY IS EMPLOYED TO PROTECT THE CONFIDENTIALITY OF CUI



Policy	Security Setting
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	Posix
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled

[A] FIPS-VALIDATED CRYPTOGRAPHY IS EMPLOYED TO PROTECT THE CONFIDENTIALITY OF CUI



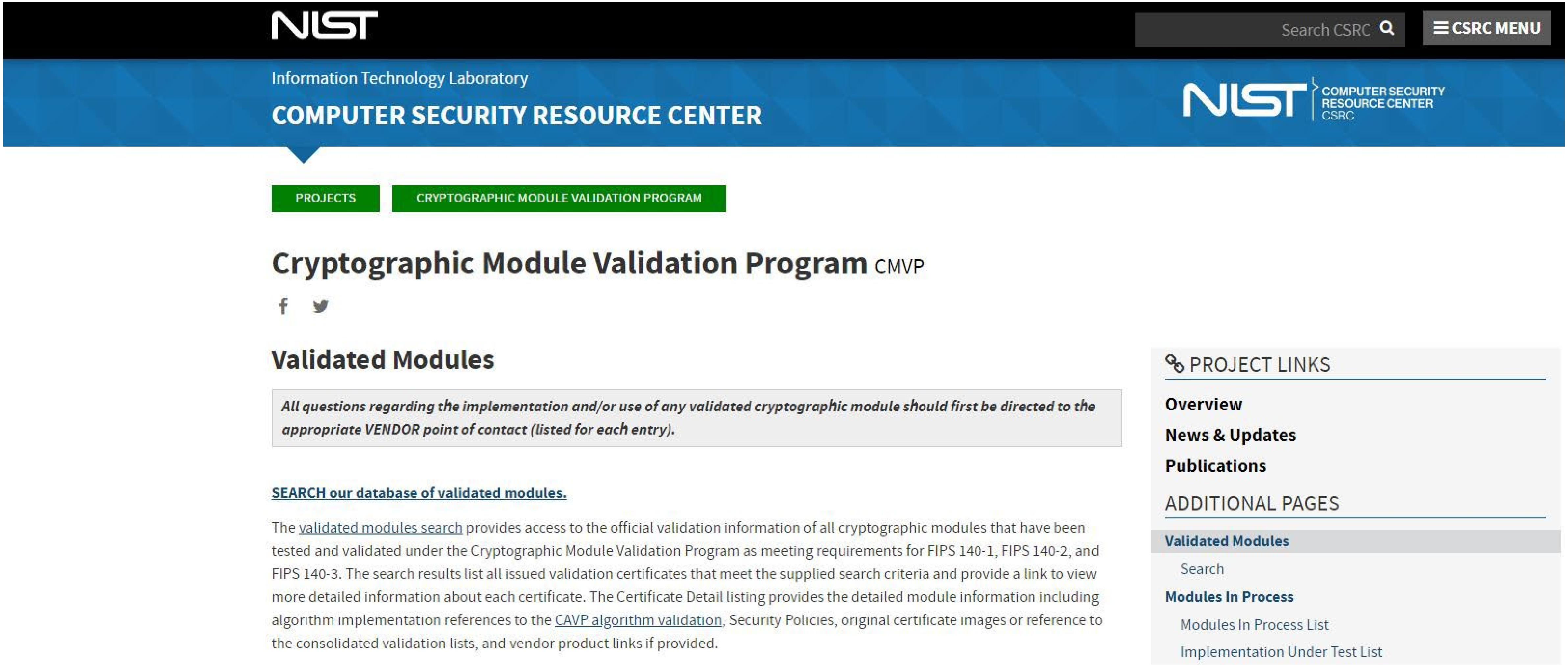
```
Connected

Neo-kvm35 # config system fips-cc

Neo-kvm35 (fips-cc) # set
entropy-token    Enable/disable/dynamic entropy token.

Neo-kvm35 (fips-cc) # set
```

PUBLIC
Public Release Authorized


NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PROJECTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

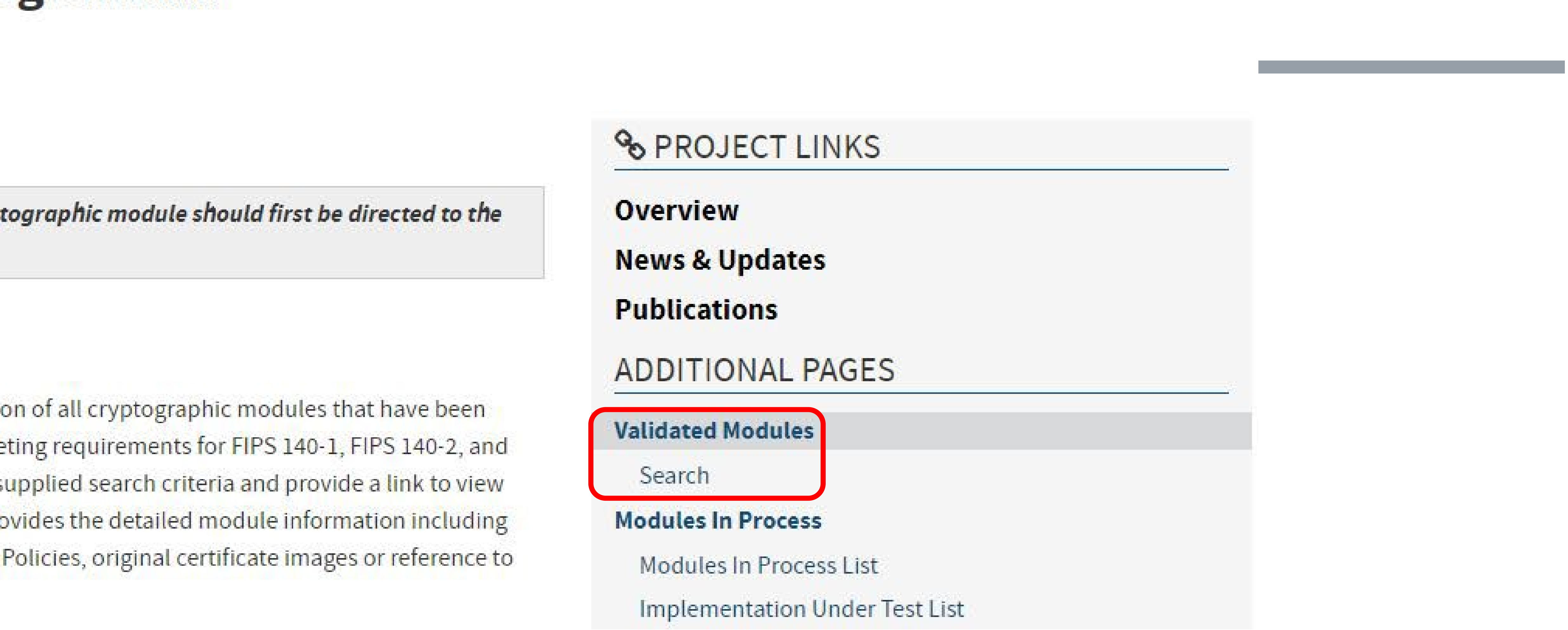
Cryptographic Module Validation Program CMVP

Validated Modules

All questions regarding the implementation and/or use of any validated cryptographic module should first be directed to the appropriate VENDOR point of contact (listed for each entry).

SEARCH our database of validated modules.

The validated modules search provides access to the official validation information of all cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS 140-1, FIPS 140-2, and FIPS 140-3. The search results list all issued validation certificates that meet the supplied search criteria and provide a link to view more detailed information about each certificate. The Certificate Detail listing provides the detailed module information including algorithm implementation references to the CAVP algorithm validation, Security Policies, original certificate images or reference to the consolidated validation lists, and vendor product links if provided.



tographic module should first be directed to the

on of all cryptographic modules that have been
eting requirements for FIPS 140-1, FIPS 140-2, and
supplied search criteria and provide a link to view
ovides the detailed module information including
Policies, original certificate images or reference to

PROJECT LINKS

Overview

News & Updates

Publications

ADDITIONAL PAGES

Validated Modules

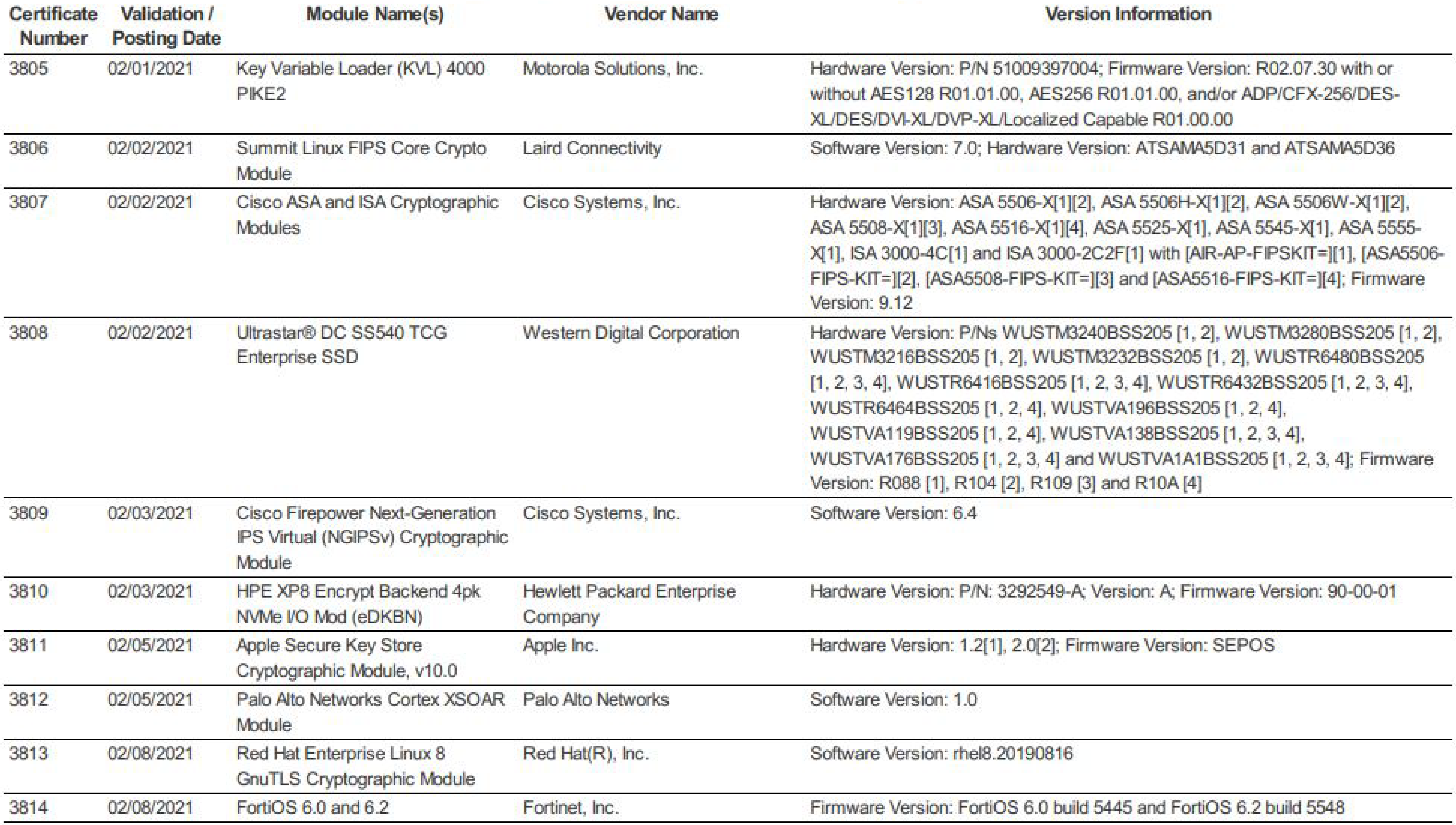
Search

Modules In Process

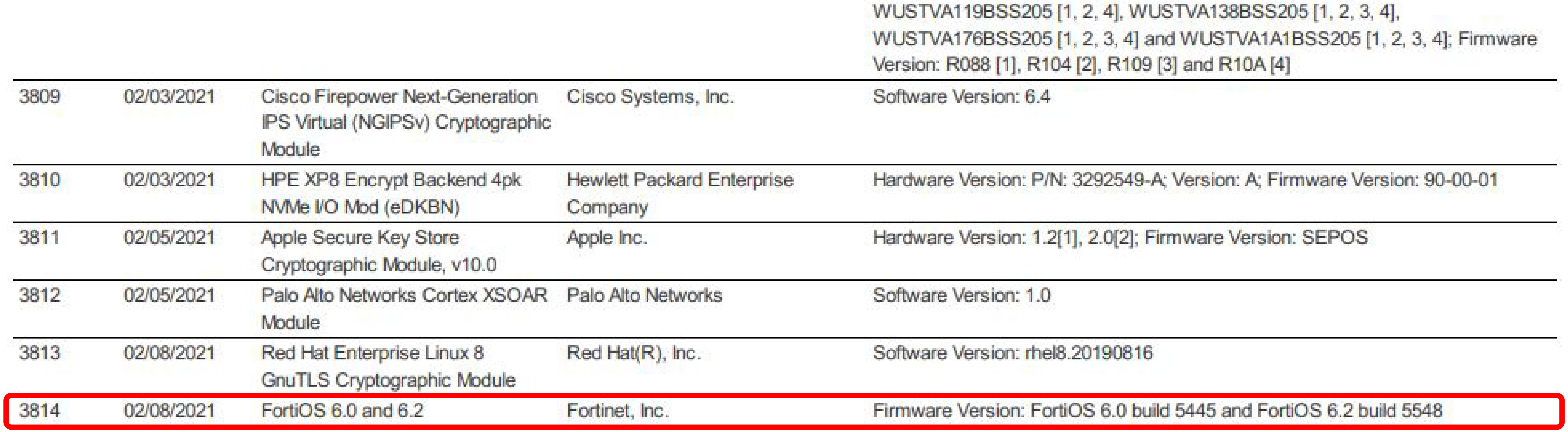
Modules In Process List

Implementation Under Test List

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

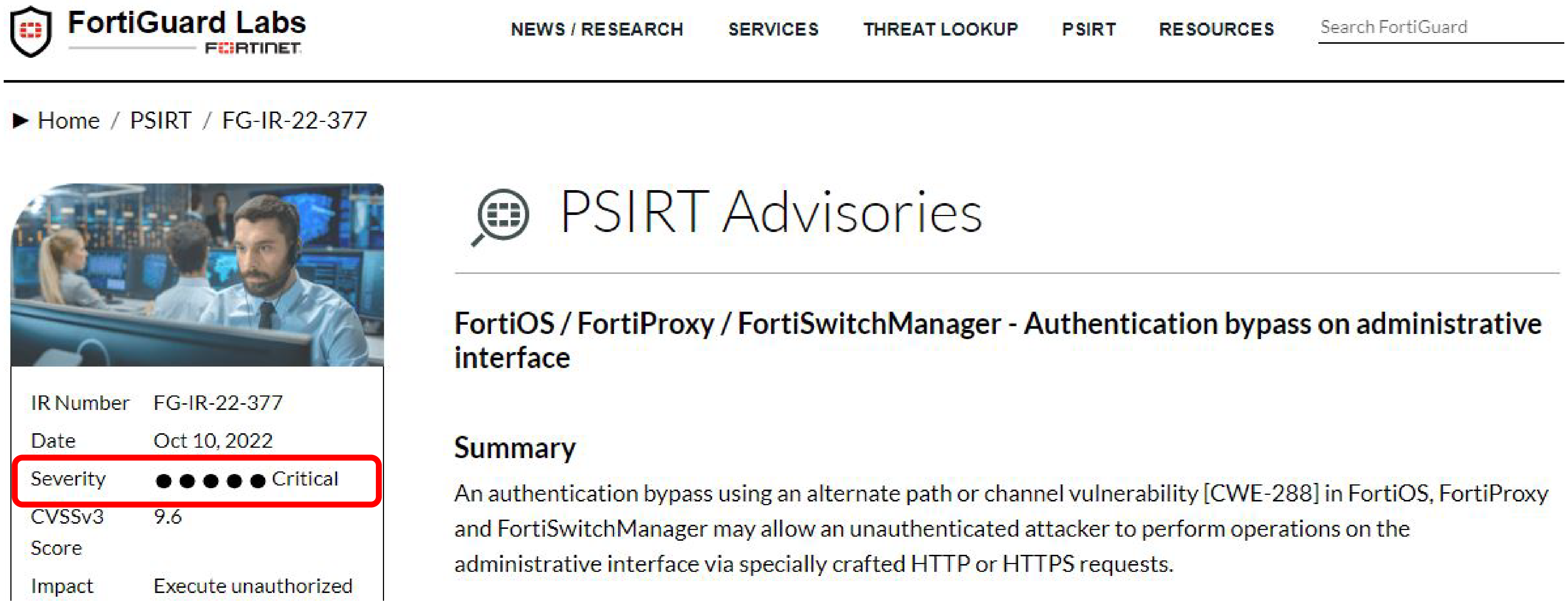


Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3805	02/01/2021	Key Variable Loader (KVL) 4000 PIKE2	Motorola Solutions, Inc.	Hardware Version: P/N 51009397004; Firmware Version: R02.07.30 with or without AES128 R01.01.00, AES256 R01.01.00, and/or ADP/CFX-256/DES-XL/DES/DVI-XL/DVP-XL/Localized Capable R01.00.00
3806	02/02/2021	Summit Linux FIPS Core Crypto Module	Laird Connectivity	Software Version: 7.0; Hardware Version: ATSAMA5D31 and ATSAMA5D36
3807	02/02/2021	Cisco ASA and ISA Cryptographic Modules	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1][2], ASA 5506H-X[1][2], ASA 5506W-X[1][2], ASA 5508-X[1][3], ASA 5516-X[1][4], ASA 5525-X[1], ASA 5545-X[1], ASA 5555-X[1], ISA 3000-4C[1] and ISA 3000-2C2F[1] with [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3] and [ASA5516-FIPS-KIT=][4]; Firmware Version: 9.12
3808	02/02/2021	Ultrastar® DC SS540 TCG Enterprise SSD	Western Digital Corporation	Hardware Version: P/Ns WUSTM3240BSS205 [1, 2], WUSTM3280BSS205 [1, 2], WUSTM3216BSS205 [1, 2], WUSTM3232BSS205 [1, 2], WUSTR6480BSS205 [1, 2, 3, 4], WUSTR6416BSS205 [1, 2, 3, 4], WUSTR6432BSS205 [1, 2, 3, 4], WUSTR6464BSS205 [1, 2, 4], WUSTVA196BSS205 [1, 2, 4], WUSTVA119BSS205 [1, 2, 4], WUSTVA138BSS205 [1, 2, 3, 4], WUSTVA176BSS205 [1, 2, 3, 4] and WUSTVA1A1BSS205 [1, 2, 3, 4]; Firmware Version: R088 [1], R104 [2], R109 [3] and R10A [4]
3809	02/03/2021	Cisco Firepower Next-Generation IPS Virtual (NGIPSv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.4
3810	02/03/2021	HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN)	Hewlett Packard Enterprise Company	Hardware Version: P/N: 3292549-A; Version: A; Firmware Version: 90-00-01
3811	02/05/2021	Apple Secure Key Store Cryptographic Module, v10.0	Apple Inc.	Hardware Version: 1.2[1], 2.0[2]; Firmware Version: SEPOS
3812	02/05/2021	Palo Alto Networks Cortex XSOAR Module	Palo Alto Networks	Software Version: 1.0
3813	02/08/2021	Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190816
3814	02/08/2021	FortiOS 6.0 and 6.2	Fortinet, Inc.	Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548



				WUSTVA119BSS205 [1, 2, 4], WUSTVA138BSS205 [1, 2, 3, 4], WUSTVA176BSS205 [1, 2, 3, 4] and WUSTVA1A1BSS205 [1, 2, 3, 4]; Firmware Version: R088 [1], R104 [2], R109 [3] and R10A [4]
3809	02/03/2021	Cisco Firepower Next-Generation IPS Virtual (NGIPSv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.4
3810	02/03/2021	HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN)	Hewlett Packard Enterprise Company	Hardware Version: P/N: 3292549-A; Version: A; Firmware Version: 90-00-01
3811	02/05/2021	Apple Secure Key Store Cryptographic Module, v10.0	Apple Inc.	Hardware Version: 1.2[1], 2.0[2]; Firmware Version: SEPOS
3812	02/05/2021	Palo Alto Networks Cortex XSOAR Module	Palo Alto Networks	Software Version: 1.0
3813	02/08/2021	Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190816
3814	02/08/2021	FortiOS 6.0 and 6.2	Fortinet, Inc.	Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI



FortiGuard Labs
FORTINET

NEWS / RESEARCH SERVICES THREAT LOOKUP PSIRT RESOURCES Search FortiGuard

▶ Home / PSIRT / FG-IR-22-377

PSIRT Advisories

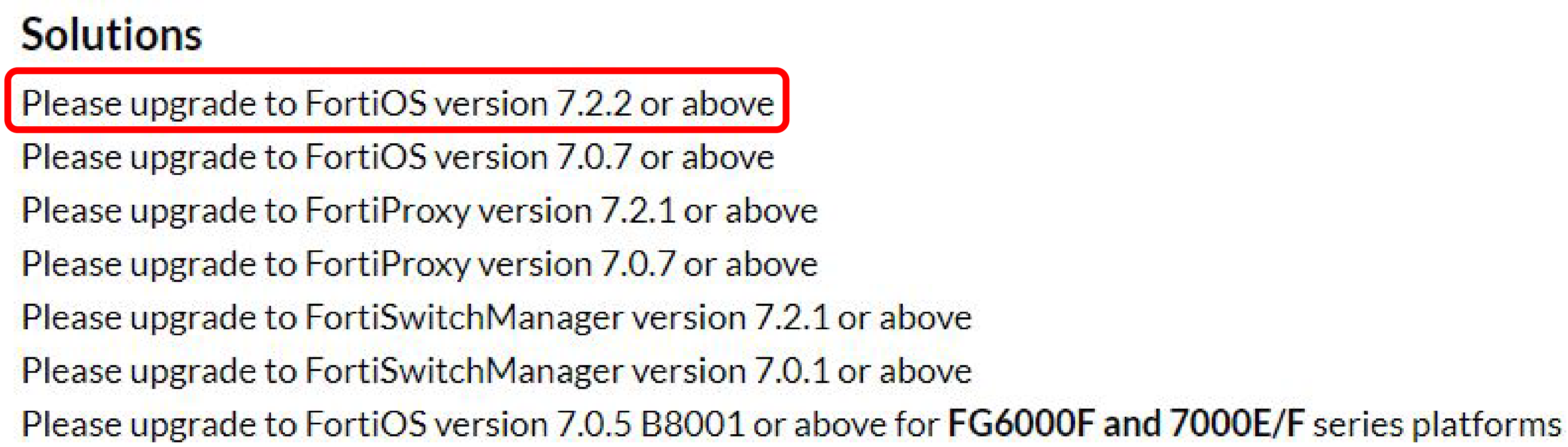
FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface

IR Number	FG-IR-22-377
Date	Oct 10, 2022
Severity	●●●●● Critical
CVSSv3 Score	9.6
Impact	Execute unauthorized

Summary

An authentication bypass using an alternate path or channel vulnerability [CWE-288] in FortiOS, FortiProxy and FortiSwitchManager may allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI



Solutions

Please upgrade to FortiOS version 7.2.2 or above

Please upgrade to FortiOS version 7.0.7 or above

Please upgrade to FortiProxy version 7.2.1 or above

Please upgrade to FortiProxy version 7.0.7 or above

Please upgrade to FortiSwitchManager version 7.2.1 or above

Please upgrade to FortiSwitchManager version 7.0.1 or above

Please upgrade to FortiOS version 7.0.5 B8001 or above for **FG6000F and 7000E/F** series platforms

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI

?

3.13.11 – EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI

DOD PROCUREMENT TOOLBOX

- *Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case. For example:*
  - *- It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines)*
  - *- Applying a necessary security patch can "invalidate" FIPS validated encryption (Requirement 3.13.11) since the encryption module "with the patch" has not been validated by NIST*
  - *- Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer*
  - *- How should a contractor deal with situations such as these?*

DOD PROCUREMENT TOOLBOX

- *Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case. For example:*
  - *- It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines)*
  - *- Applying a necessary security patch can “invalidate” FIPS validated encryption (Requirement 3.13.11) since the encryption module “with the patch” has not been validated by NIST*
  - *- Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer*
  - *- How should a contractor deal with situations such as these?*

DOD PROCUREMENT TOOLBOX

- *A59: The requirement at DFARS clause 252.204-7012(b)(2)(i) to implement, at a minimum, the security requirements in NIST SP 800-171, is not intended to imply that there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short- or long-term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii) and DFARS clause 252.204-7012(b)(2)(ii).*

DOD PROCUREMENT TOOLBOX

- *A59: The requirement at DFARS clause 252.204-7012(b)(2)(i) to implement, at a minimum, the security requirements in NIST SP 800-171, is not intended to imply that there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short- or long-term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii) and DFARS clause 252.204-7012(b)(2)(ii).*

DOD PROCUREMENT TOOLBOX

- *A59: The contractor should address situations such as those listed above in accordance with the NIST SP 800-171 security requirements that follow:*
  - *- 3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI;*
  - *- 3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls;*
  - *- 3.12.2, Security Assessment: Requires the contractor to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;"*
  - *- 3.12.3, Security Assessment: Monitor security controls in an ongoing basis to ensure the continued effectiveness of the controls;" and*
  - *- 3.12.4, System security plan: Requires the contractor to "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."*

DOD PROCUREMENT TOOLBOX

- *A59: The contractor should address situations such as those listed above in accordance with the NIST SP 800-171 security requirements that follow:*
  - *- 3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI;*
  - *- 3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls;*
  - *- 3.12.2, Security Assessment: Requires the contractor to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;"*
  - *- 3.12.3, Security Assessment: Monitor security controls in an ongoing basis to ensure the continued effectiveness of the controls;" and*
  - *- 3.12.4, System security plan: Requires the contractor to "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."*

FIPS-VALIDATED CRYPTOGRAPHY KEY POINTS

- *If your FIPS-validated version is vulnerable*
  - Conduct risk & security assessment
  - Coordinate with the vendor
  - Track with your Plan of Action & Milestones (POA&M)
- *If your patch version is not validated*
  - Coordinate with the vendor
  - Track with your Plan of Action & Milestones (POA&M)
- *If your product has been sunset*
  - Coordinate with the vendor or replace
  - Track with your Plan of Action & Milestones (POA&M)

14		$ 1 MILLION
13		$ 500,000
12		$ 250,000
11		$ 100,000
10		$ 50,000
9		$ 30,000
8		$ 20,000
7		$ 10,000
6		$ 7,000
5		$ 5,000
4		$ 3,000
3	◆	$ 2,000
2	◆	$ 1,000
1	◆	$ 500

WHO WANTS TO BE A MILLIONAIRE SPECIAL EDITIONS WHO WANTS TO BE A

$ 3000

Of the available options, which cryptography is required to protect controlled unclassified information (CUI)?

A: Regular cryptography

B: Irregular cryptography

C: United States cryptography

D: FIPS-validated cryptography

$ 3000

Of the available options, which cryptography is required to protect controlled unclassified information (CUI)?

A: Regular cryptography

B: Irregular cryptography

C: United States cryptography

[✓ D: FIPS-validated cryptography]

14		$ 1 MILLION
13		$ 500,000
12		$ 250,000
11		$ 100,000
10		$ 50,000
9		$ 30,000
8		$ 20,000
7		$ 10,000
6		$ 7,000
5		$ 5,000
4	◆	$ 3,000
3	◆	$ 2,000
2	◆	$ 1,000
1	◆	$ 500

WHO WANTS TO BE A MILLIONAIRE SPECIAL EDITIONS WHO WANTS TO BE A

$ 5000

What is the purpose of FIPS-validated encryption?

A: To protect the integrity of CUI

B: To protect the availability of CUI

C: To protect the security of CUI

D: To protect the confidentiality of CUI

$ 5000

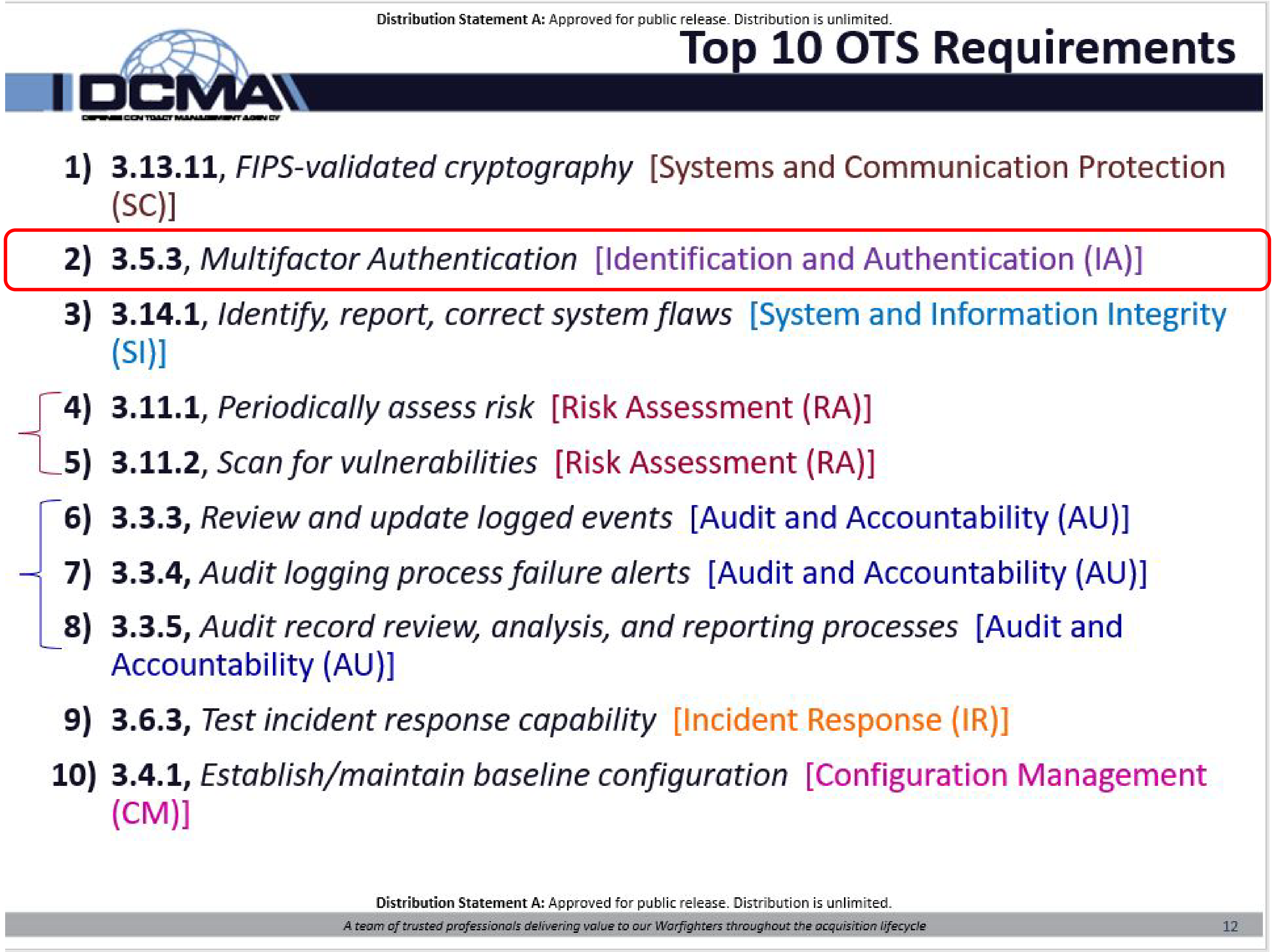
What is the purpose of FIPS-validated encryption?

A: To protect the integrity of CUI

B: To protect the availability of CUI

C: To protect the security of CUI

D: To protect the confidentiality of CUI



Distribution Statement A: Approved for public release. Distribution is unlimited.

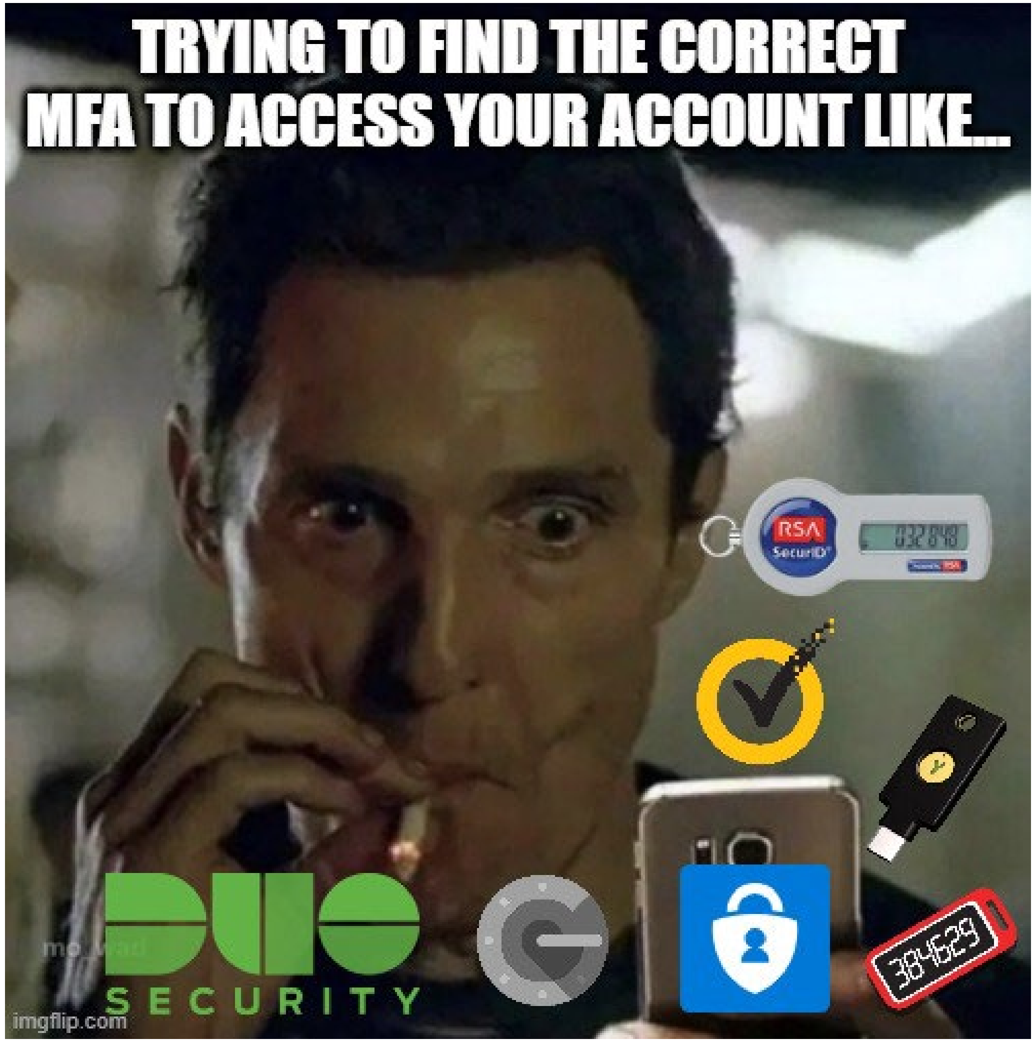
DCMA

Top 10 OTS Requirements

1) **3.13.11**, *FIPS-validated cryptography* [Systems and Communication Protection (SC)]
2) **3.5.3**, *Multifactor Authentication* [Identification and Authentication (IA)]
3) **3.14.1**, *Identify, report, correct system flaws* [System and Information Integrity (SI)]
4) **3.11.1**, *Periodically assess risk* [Risk Assessment (RA)]
5) **3.11.2**, *Scan for vulnerabilities* [Risk Assessment (RA)]
6) **3.3.3,** *Review and update logged events* [Audit and Accountability (AU)]
7) **3.3.4,** *Audit logging process failure alerts* [Audit and Accountability (AU)]
8) **3.3.5,** *Audit record review, analysis, and reporting processes* [Audit and Accountability (AU)]
9) **3.6.3,** *Test incident response capability* [Incident Response (IR)]
10) **3.4.1,** *Establish/maintain baseline configuration* [Configuration Management (CM)]

Distribution Statement A: Approved for public release. Distribution is unlimited.

3.5.3 – USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS


TRYING TO FIND THE CORRECT MFA TO ACCESS YOUR ACCOUNT LIKE...
RSA SecurID
032848
DUO SECURITY
384629
imgflip.com

3.5.3 – USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

- *Determine if:*
  - *[a] Privileged accounts are identified*
  - *[b] Multifactor authentication is implemented for local access to privileged accounts*
  - *[c] Multifactor authentication is implemented for network access to privileged accounts*
  - *[d] Multifactor authentication is implemented for network access to non-privileged accounts*

3.5.3 – USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

- *Determine if:*
  - *[a] Privileged accounts are identified*
  - *[b] Multifactor authentication is implemented for local access to privileged accounts*
  - *[c] Multifactor authentication is implemented for network access to privileged accounts*
  - *[d] Multifactor authentication is implemented for network access to non-privileged accounts*

[A] PRIVILEGED ACCOUNTS ARE IDENTIFIED

NIST SP 800-171 Glossary

- Privileged Account
  - A 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

[A] PRIVILEGED ACCOUNTS ARE IDENTIFIED

NIST SP 800-171 Glossary

- Privileged Account
  - A 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

[A] PRIVILEGED ACCOUNTS ARE IDENTIFIED

- Examples of privileged accounts:
  - Firewall administrator accounts
  - Local administrator accounts
  - DNS administrator accounts

WatchGuard®

cisco

FORTINET®

cisco

Cisco Umbrella

SOPHOS

[A] PRIVILEGED ACCOUNTS ARE IDENTIFIED

- Potential solutions to identify privileged accounts:
  - Employee Onboarding Checklist
  - Privileged User Form

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

3.5.3 – USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

- *Determine if:*
  - *[a] Privileged accounts are identified*
  - *[b] Multifactor authentication is implemented for local access to privileged accounts*
  - *[c] Multifactor authentication is implemented for network access to privileged accounts*
  - *[d] Multifactor authentication is implemented for network access to non-privileged accounts*

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS

- *Discussion: Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS

- ***Discussion***: *Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS

Something you have (e.g., one-time password (OTP) generating device like a fob, smart-card, or a mobile app on a smart phone

Something you know (e.g., password, PIN)

Something you are (e.g., a biometric like a fingerprint or iris)

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS

- *Discussion*: *Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS
DOD PROCUREMENT TOOLBOX

- *Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by “multifactor authentication”?*
- *“For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA.”*

[B] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR LOCAL ACCESS TO PRIVILEGED ACCOUNTS
DOD PROCUREMENT TOOLBOX

- *Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication"?*
- *"For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA."*

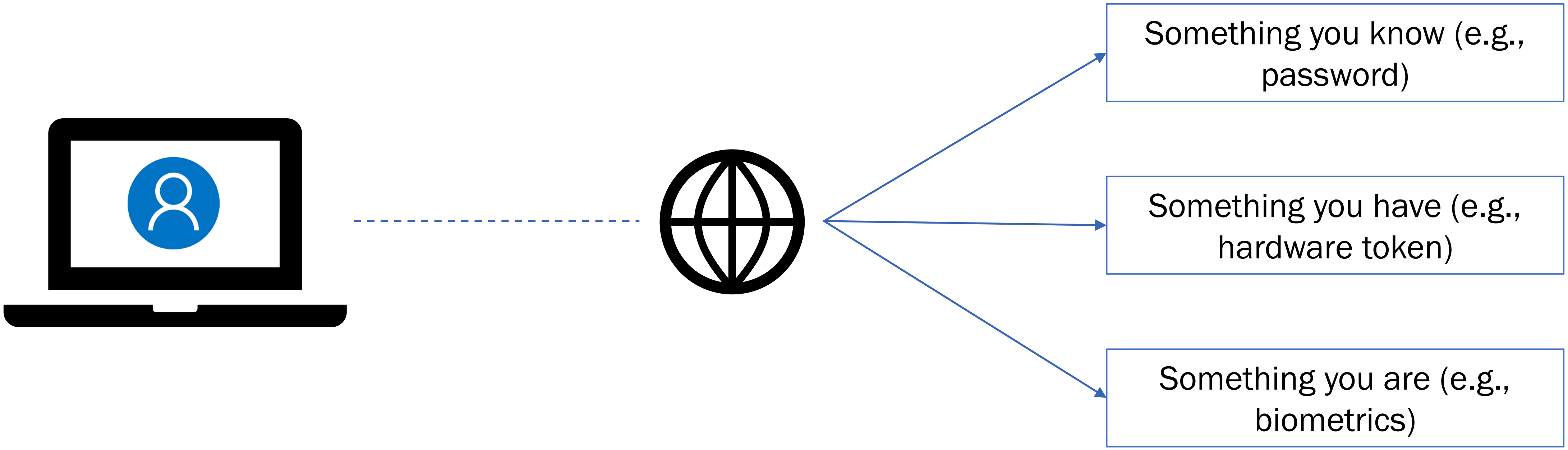
3.5.3 – USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

- *Determine if:*
  - *[a] Privileged accounts are identified*
  - *[b] Multifactor authentication is implemented for local access to privileged accounts*
  - *[c] Multifactor authentication is implemented for network access to privileged accounts*
  - *[d] Multifactor authentication is implemented for network access to non-privileged accounts*

[C] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO PRIVILEGED ACCOUNTS
[D] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

- *Discussion*: *Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[C] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO PRIVILEGED ACCOUNTS
[D] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

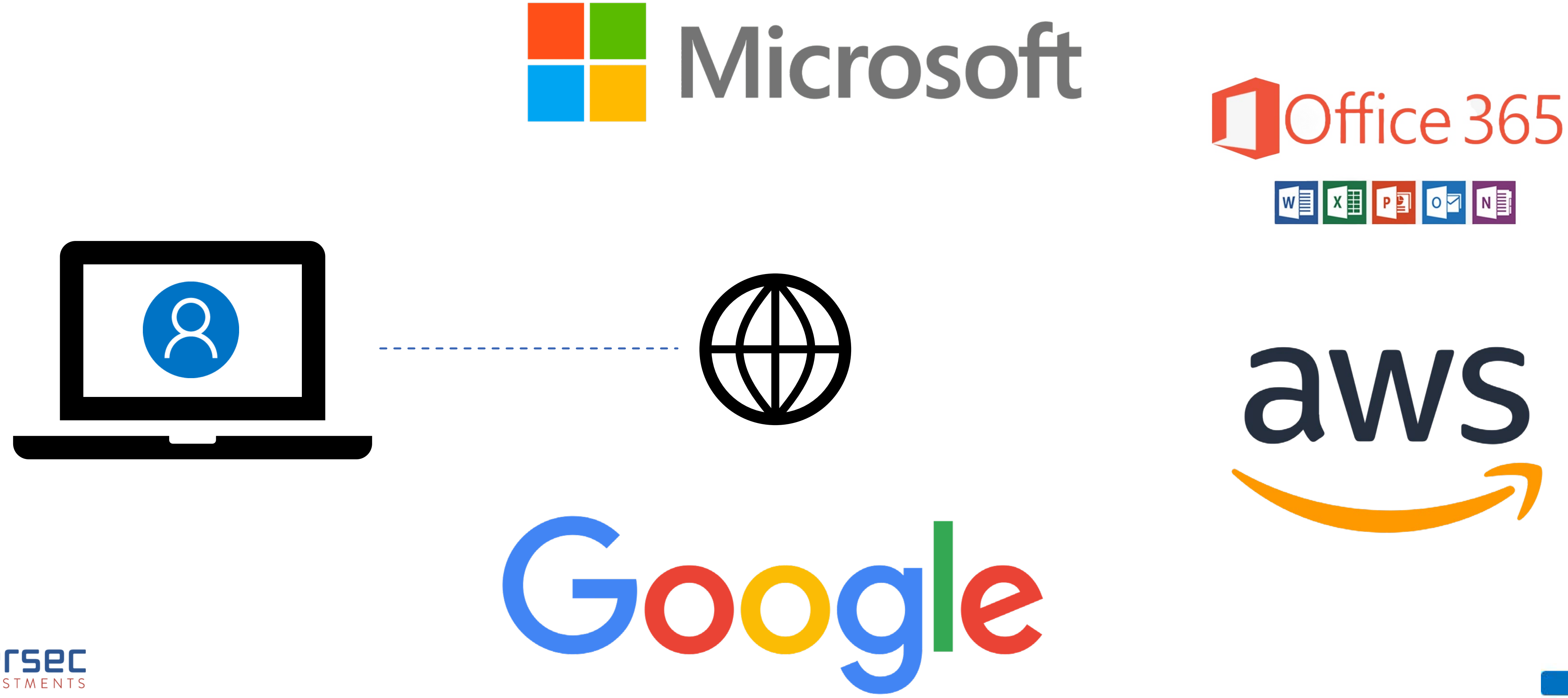


Something you know (e.g., password)

Something you have (e.g., hardware token)

Something you are (e.g., biometrics)

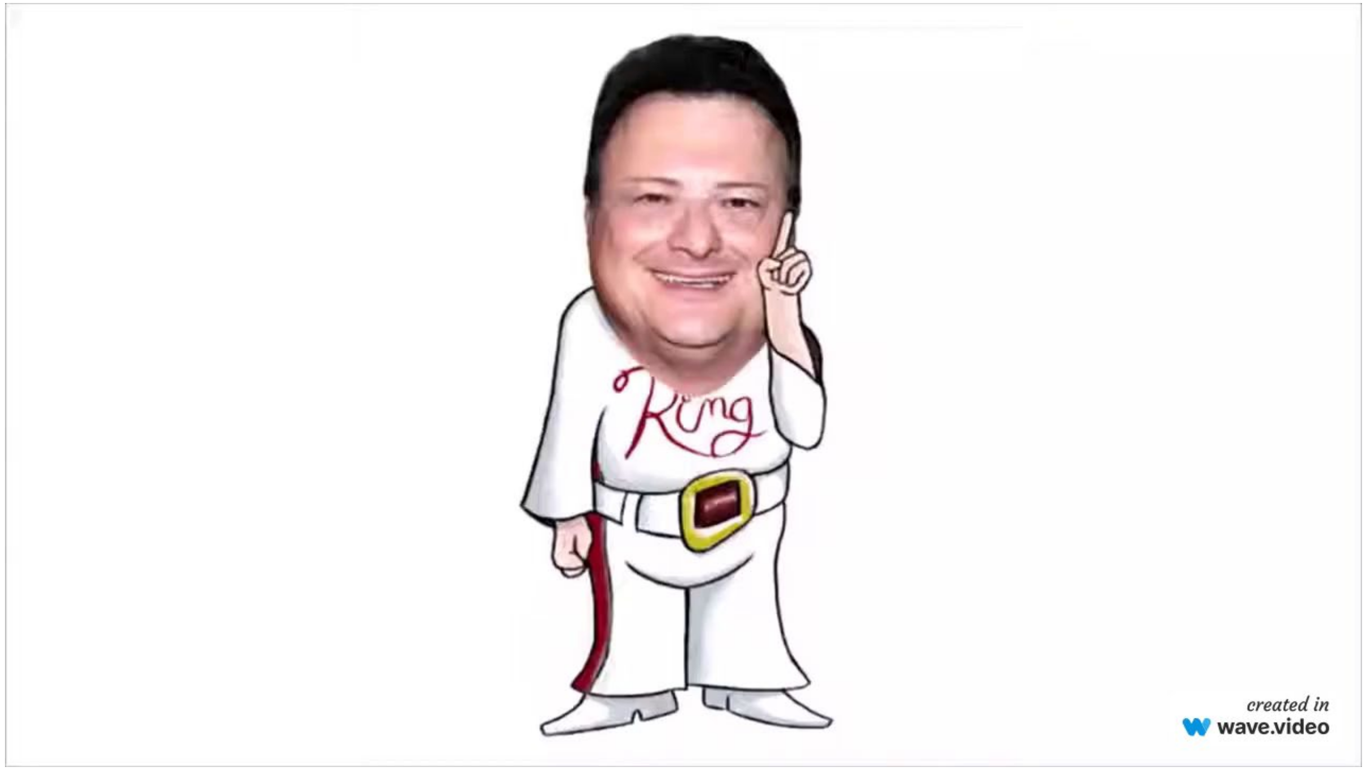
[C] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO PRIVILEGED ACCOUNTS
[D] MULTIFACTOR AUTHENTICATION IS IMPLEMENTED FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS



DOD PROCUREMENT TOOLBOX

- *Q81: Security Requirement 3.5.3 – Can one of the factors in multifactor authentication be where you are (e.g., within a controlled access facility)?*

DOD PROCUREMENT TOOLBOX



DOD PROCUREMENT TOOLBOX

- *A81: No. Multifactor requires at least two of the following three factors: what you know (e.g., secret password), what you are (e.g., fingerprint), and what you have (e.g., PKI certificate on smartcard, OTP device). Each of these factors is unique to the individual being authenticated. Where you are, even in a controlled access facility is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated.*

DOD PROCUREMENT TOOLBOX

- *A81: No. Multifactor requires at least two of the following three factors: what you know (e.g., secret password), what you are (e.g., fingerprint), and what you have (e.g., PKI certificate on smartcard, OTP device). Each of these factors is unique to the individual being authenticated. Where you are, even in a controlled access facility is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated.*

DOD PROCUREMENT TOOLBOX

- *A81*: *No. Multifactor requires at least two of the following three factors: what you know (e.g., secret password), what you are (e.g., fingerprint), and what you have (e.g., PKI certificate on smartcard, OTP device). Each of these factors is unique to the individual being authenticated. Where you are, even in a controlled access facility is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated.*

DOD PROCUREMENT TOOLBOX

- *Q84: Security Requirement 3.5.3 – What if I have covered defense information on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?*

DOD PROCUREMENT TOOLBOX

DOD PROCUREMENT TOOLBOX

- *A84: No, that is covered under a separate security requirement, 3.1.19 - Encrypt CUI on mobile devices. As noted above, the multifactor authentication requirement applies to an information system, and a mobile device in not considered an "information system." But, if there will be covered defense information on a mobile device, it must be encrypted. This can be done by encrypting all the data on the device (as is typically done on a laptop, and is available with recent iOS devices and some Android/Windows devices) or via a container (like the Good app, which is available for iOS (iPhone, iPad), Android, Windows; Blackberry's Secure Work Space for iOS and Android; etc.) to separate the covered defense information from the other information on the phone (or company information from personal information if employing a bring your own device (BYOD) approach). Care should be taken to ensure the encryption module is FIPS-validated for either the whole device or container. Information that is independently and appropriately encrypted (e.g., an e-mail encrypted with a PKI certificate) is self-protecting and need not be double-encrypted.*

DOD PROCUREMENT TOOLBOX

- *A84: No, that is covered under a separate security requirement, 3.1.19 - Encrypt CUI on mobile devices. As noted above, the multifactor authentication requirement applies to an information system, and a mobile device in not considered an “information system.” But, if there will be covered defense information on a mobile device, it must be encrypted. This can be done by encrypting all the data on the device (as is typically done on a laptop, and is available with recent iOS devices and some Android/Windows devices) or via a container (like the Good app, which is available for iOS (iPhone, iPad), Android, Windows; Blackberry’s Secure Work Space for iOS and Android; etc.) to separate the covered defense information from the other information on the phone (or company information from personal information if employing a bring your own device (BYOD) approach). Care should be taken to ensure the encryption module is FIPS-validated for either the whole device or container. Information that is independently and appropriately encrypted (e.g., an e-mail encrypted with a PKI certificate) is self-protecting and need not be double-encrypted.*

14		$ 1 MILLION
13		$ 500,000
12		$ 250,000
11		$ 100,000
10		$ 50,000
9		$ 30,000
8		$ 20,000
7		$ 10,000
6		$ 7,000
5	◆	$ 5,000
4	◆	$ 3,000
3	◆	$ 2,000
2	◆	$ 1,000
1	◆	$ 500

$ 7000

In order to achieve the intent of multifactor authentication, at least how many factors must be used?

A: Two

B: Three

C: One

D
: Four

WHO WANTS TO BE A MILLIONAIRE SPECIAL EDITIONS WHO WANTS TO BE A

$ 7000

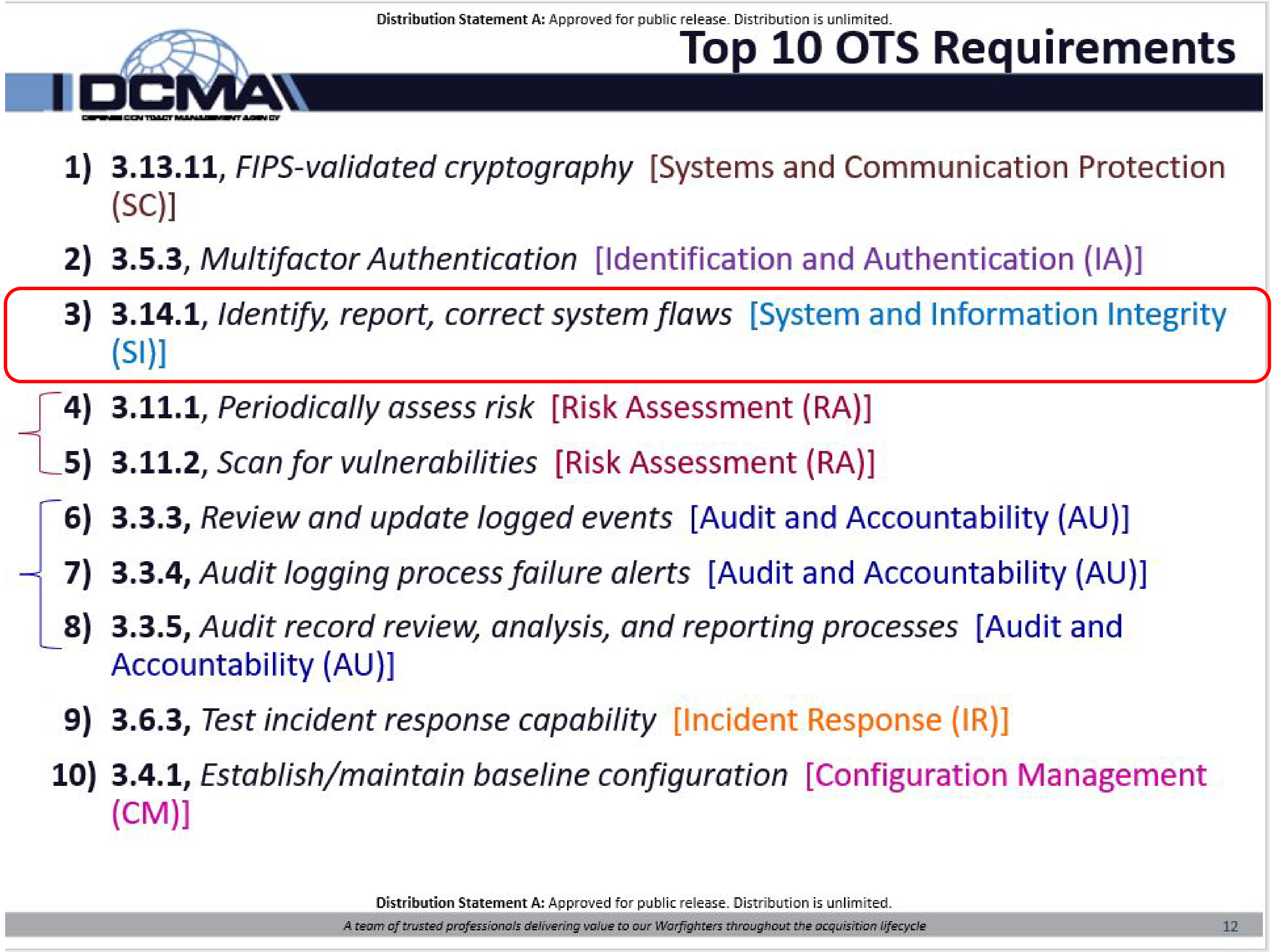
In order to achieve the intent of multifactor authentication, at least how many factors must be used?

[✓ A: Two]

B: Three

C: One

D: Four



Distribution Statement A: Approved for public release. Distribution is unlimited.

Top 10 OTS Requirements

DCMA

1) **3.13.11**, *FIPS-validated cryptography* [Systems and Communication Protection (SC)]
2) **3.5.3**, *Multifactor Authentication* [Identification and Authentication (IA)]
3) **3.14.1**, *Identify, report, correct system flaws* [System and Information Integrity (SI)]
4) **3.11.1**, *Periodically assess risk* [Risk Assessment (RA)]
5) **3.11.2**, *Scan for vulnerabilities* [Risk Assessment (RA)]
6) **3.3.3,** *Review and update logged events* [Audit and Accountability (AU)]
7) **3.3.4,** *Audit logging process failure alerts* [Audit and Accountability (AU)]
8) **3.3.5,** *Audit record review, analysis, and reporting processes* [Audit and Accountability (AU)]
9) **3.6.3,** *Test incident response capability* [Incident Response (IR)]
10) **3.4.1,** *Establish/maintain baseline configuration* [Configuration Management (CM)]

Distribution Statement A: Approved for public release. Distribution is unlimited.

A team of trusted professionals delivering value to our Warfighters throughout the acquisition lifecycle

PUBLIC

Public Release Authorized

3.14.1 – IDENTIFY, REPORT, AND CORRECT SYSTEM FLAWS IN A TIMELY MANNER

- *Determine if:*
  - *[a] The time within which to identify system flaws is specified*
  - *[b] System flaws are identified within the specified time frame*
  - *[c] The time within which to report system flaws is specified*
  - *[d] System flaws are reported within the specified time frame*
  - *[e] The time within which to correct system flaws is specified*
  - *[f] System flaws are corrected within the specified time frame*

3.14.1 – IDENTIFY, REPORT, AND CORRECT SYSTEM FLAWS IN A TIMELY MANNER

- *Determine if:*
  - *[a] The time within which to identify system flaws is specified*
  - *[b] System flaws are identified within the specified time frame*
  - *[c] The time within which to report system flaws is specified*
  - *[d] System flaws are reported within the specified time frame*
  - *[e] The time within which to correct system flaws is specified*
  - *[f] System flaws are corrected within the specified time frame*

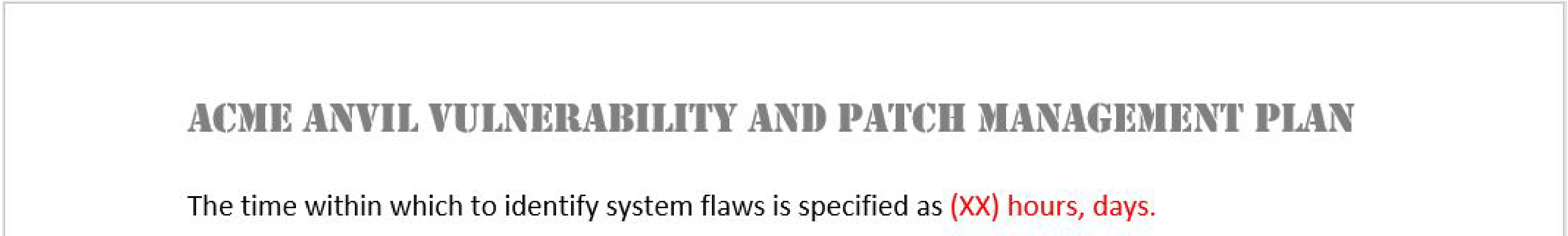
[A] THE TIME WITHIN WHICH TO IDENTIFY SYSTEM FLAWS IS SPECIFIED [B] SYSTEM FLAWS ARE IDENTIFIED WITHIN THE SPECIFIED TIME FRAME

- *Discussion: Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.*

[A] THE TIME WITHIN WHICH TO IDENTIFY SYSTEM FLAWS IS SPECIFIED
[B] SYSTEM FLAWS ARE IDENTIFIED WITHIN THE SPECIFIED TIME FRAME

- *__Discussion__: Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.*

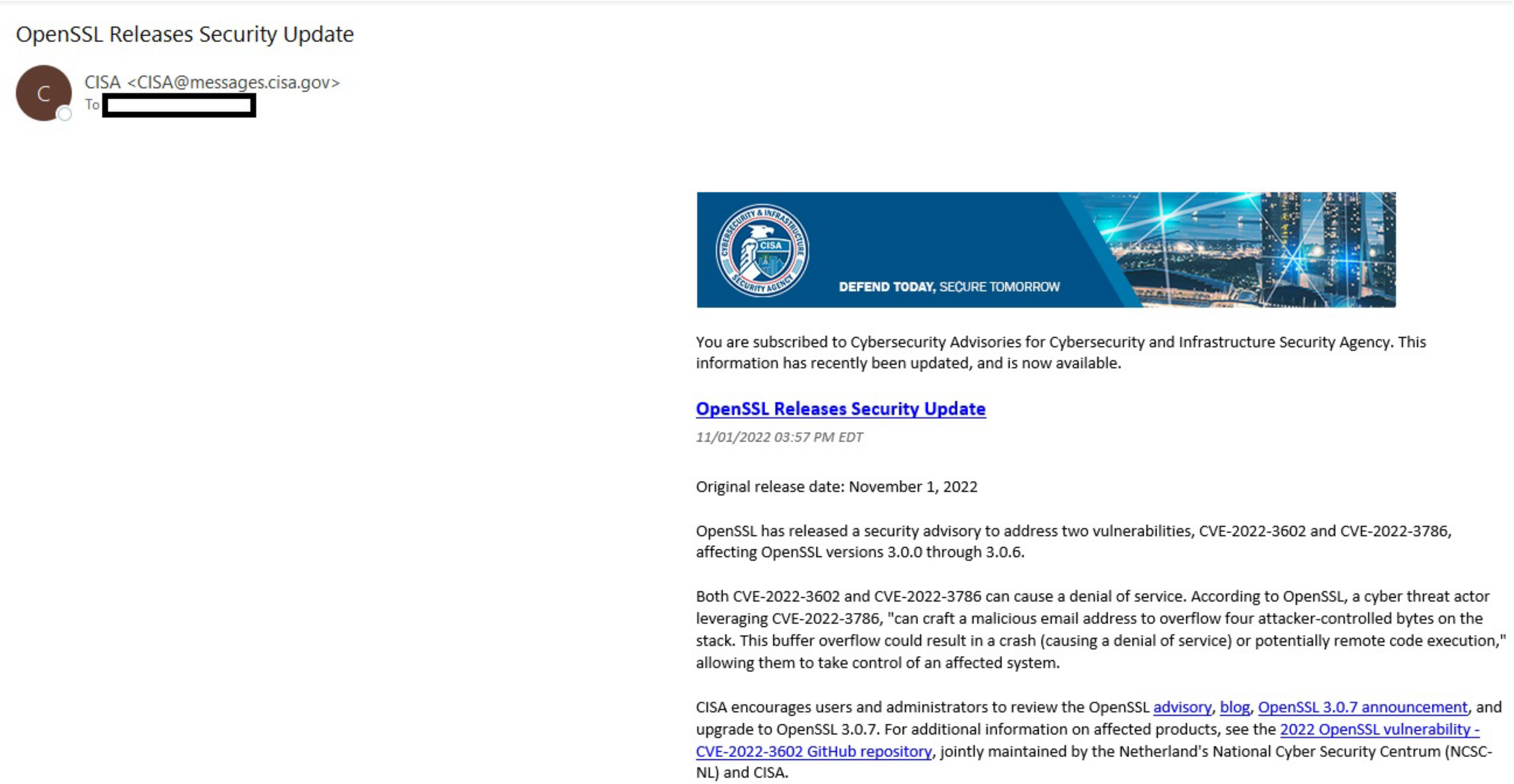
[A] THE TIME WITHIN WHICH TO IDENTIFY SYSTEM FLAWS IS SPECIFIED
[B] SYSTEM FLAWS ARE IDENTIFIED WITHIN THE SPECIFIED TIME FRAME



ACME ANVIL VULNERABILITY AND PATCH MANAGEMENT PLAN

The time within which to identify system flaws is specified as (XX) hours, days.

[A] THE TIME WITHIN WHICH TO IDENTIFY SYSTEM FLAWS IS SPECIFIED
[B] SYSTEM FLAWS ARE IDENTIFIED WITHIN THE SPECIFIED TIME FRAME



OpenSSL Releases Security Update

CISA <CISA@messages.cisa.gov>
To [redacted]

You are subscribed to Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

OpenSSL Releases Security Update

11/01/2022 03:57 PM EDT

Original release date: November 1, 2022

OpenSSL has released a security advisory to address two vulnerabilities, CVE-2022-3602 and CVE-2022-3786, affecting OpenSSL versions 3.0.0 through 3.0.6.

Both CVE-2022-3602 and CVE-2022-3786 can cause a denial of service. According to OpenSSL, a cyber threat actor leveraging CVE-2022-3786, "can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution," allowing them to take control of an affected system.

CISA encourages users and administrators to review the OpenSSL advisory, blog, OpenSSL 3.0.7 announcement, and upgrade to OpenSSL 3.0.7. For additional information on affected products, see the 2022 OpenSSL vulnerability - CVE-2022-3602 GitHub repository, jointly maintained by the Netherland's National Cyber Security Centrum (NCSC-NL) and CISA.

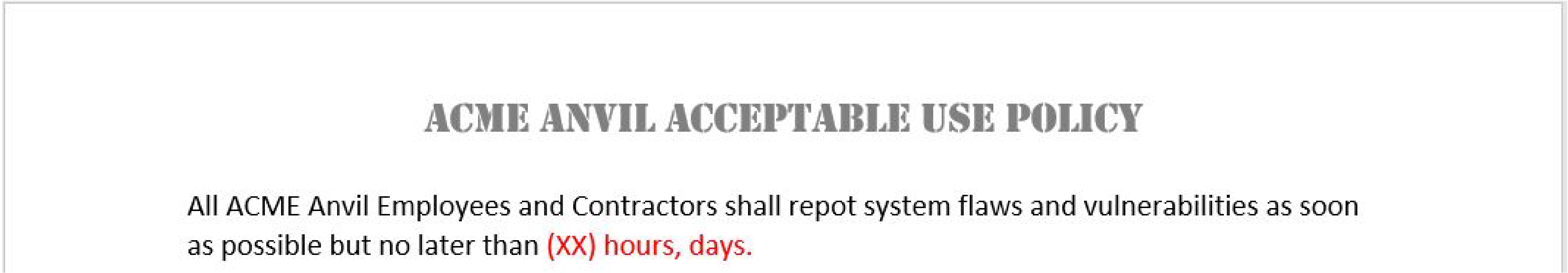
3.14.1 – IDENTIFY, REPORT, AND CORRECT SYSTEM FLAWS IN A TIMELY MANNER

- *Determine if:*
  - *[a] The time within which to identify system flaws is specified*
  - *[b] System flaws are identified within the specified time frame*
  - *[c] The time within which to report system flaws is specified*
  - *[d] System flaws are reported within the specified time frame*
  - *[e] The time within which to correct system flaws is specified*
  - *[f] System flaws are corrected within the specified time frame*

[C] THE TIME WITHIN WHICH TO REPORT SYSTEM FLAWS IS SPECIFIED
[D] SYSTEM FLAWS ARE REPORTED WITHIN THE SPECIFIED TIME FRAME

- ***Discussion***: *Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.*

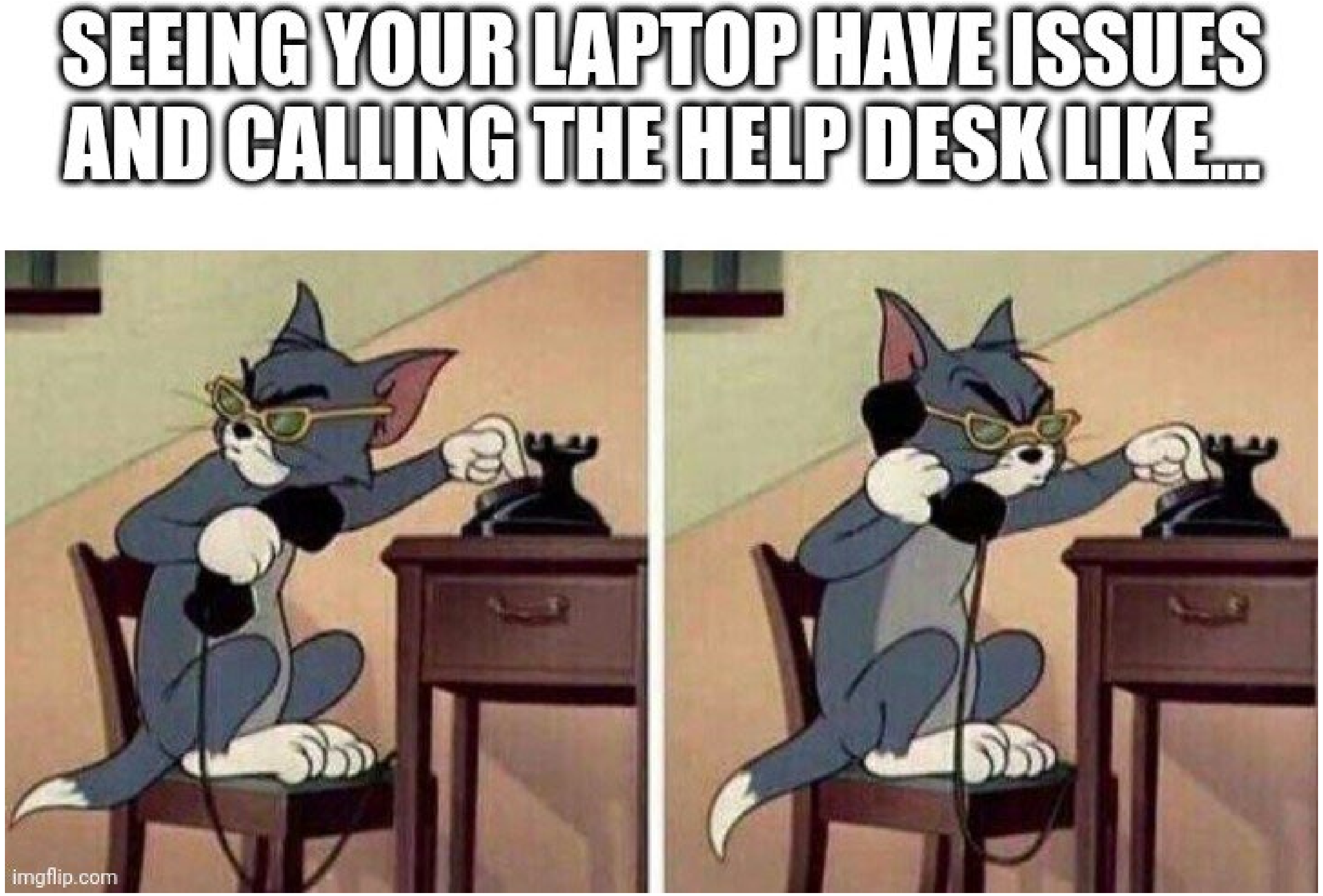
[C] THE TIME WITHIN WHICH TO REPORT SYSTEM FLAWS IS SPECIFIED
[D] SYSTEM FLAWS ARE REPORTED WITHIN THE SPECIFIED TIME FRAME



ACME ANVIL ACCEPTABLE USE POLICY

All ACME Anvil Employees and Contractors shall repot system flaws and vulnerabilities as soon as possible but no later than (XX) hours, days.

[C] THE TIME WITHIN WHICH TO REPORT SYSTEM FLAWS IS SPECIFIED
[D] SYSTEM FLAWS ARE REPORTED WITHIN THE SPECIFIED TIME FRAME


SEEING YOUR LAPTOP HAVE ISSUES
AND CALLING THE HELP DESK LIKE...
imgflip.com

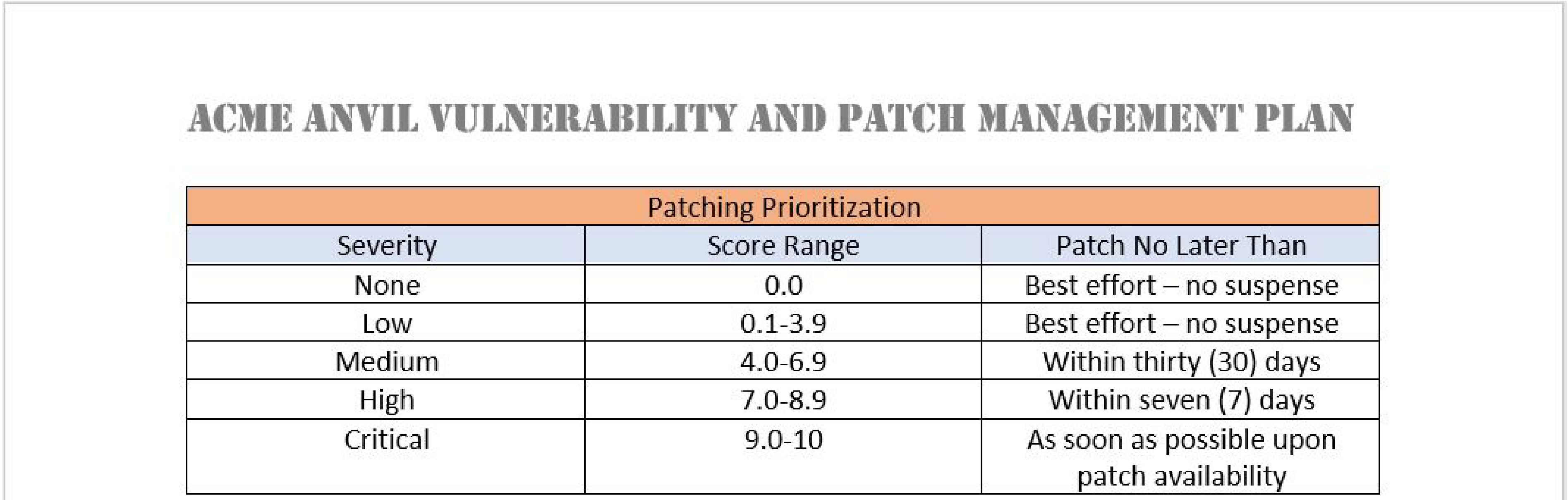
3.14.1 – IDENTIFY, REPORT, AND CORRECT SYSTEM FLAWS IN A TIMELY MANNER

- *Determine if:*
  - *[a] The time within which to identify system flaws is specified*
  - *[b] System flaws are identified within the specified time frame*
  - *[c] The time within which to report system flaws is specified*
  - *[d] System flaws are reported within the specified time frame*
  - *[e] The time within which to correct system flaws is specified*
  - *[f] System flaws are corrected within the specified time frame*

[E] THE TIME WITHIN WHICH TO CORRECT SYSTEM FLAWS IS SPECIFIED
[F] SYSTEM FLAWS ARE CORRECTED WITHIN THE SPECIFIED TIME FRAME

- *Discussion: Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.*

[E] THE TIME WITHIN WHICH TO CORRECT SYSTEM FLAWS IS SPECIFIED
[F] SYSTEM FLAWS ARE CORRECTED WITHIN THE SPECIFIED TIME FRAME



ACME ANVIL VULNERABILITY AND PATCH MANAGEMENT PLAN

Patching Prioritization		
Severity	Score Range	Patch No Later Than
None	0.0	Best effort – no suspense
Low	0.1-3.9	Best effort – no suspense
Medium	4.0-6.9	Within thirty (30) days
High	7.0-8.9	Within seven (7) days
Critical	9.0-10	As soon as possible upon patch availability

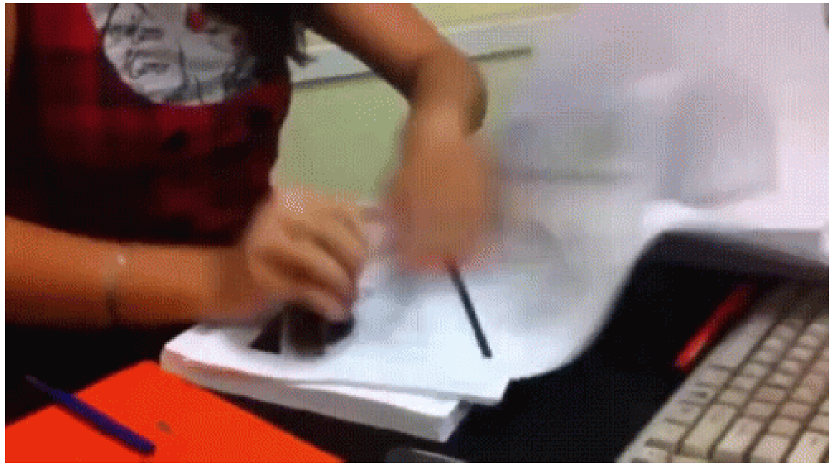
WHAT YOUR ASSESSOR WILL BE LOOKING FOR

NIST SP 800-171A POTENTIAL ASSESSMENT METHODS AND OBJECTS

- Examine
  - The process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities).
    - [SELECT FROM: Identification and Authentication Policy; Procedures addressing user identification and authentication; etc.]
- Interview
  - The process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.
    - [SELECT FROM: Personnel with system operations responsibilities, etc.]
- Test
  - The process of exercising assessment objects (i.e., activities, mechanisms under specified conditions to compare actual with expect behavior.
    - [SELECT FROM: Mechanisms supporting or implementing multifactor authentication capability]

PAY ATTENTION TO THE VERBS

Associated with Documentation	Associated with Action
Identified	Limited
Defined	Implemented
Specified	Performed



Cybersec
INVESTMENTS

PUBLIC
Public Release Authorized

NIST SP 800-171A / CMMC ASSESSMENT PROCESS (CAP)

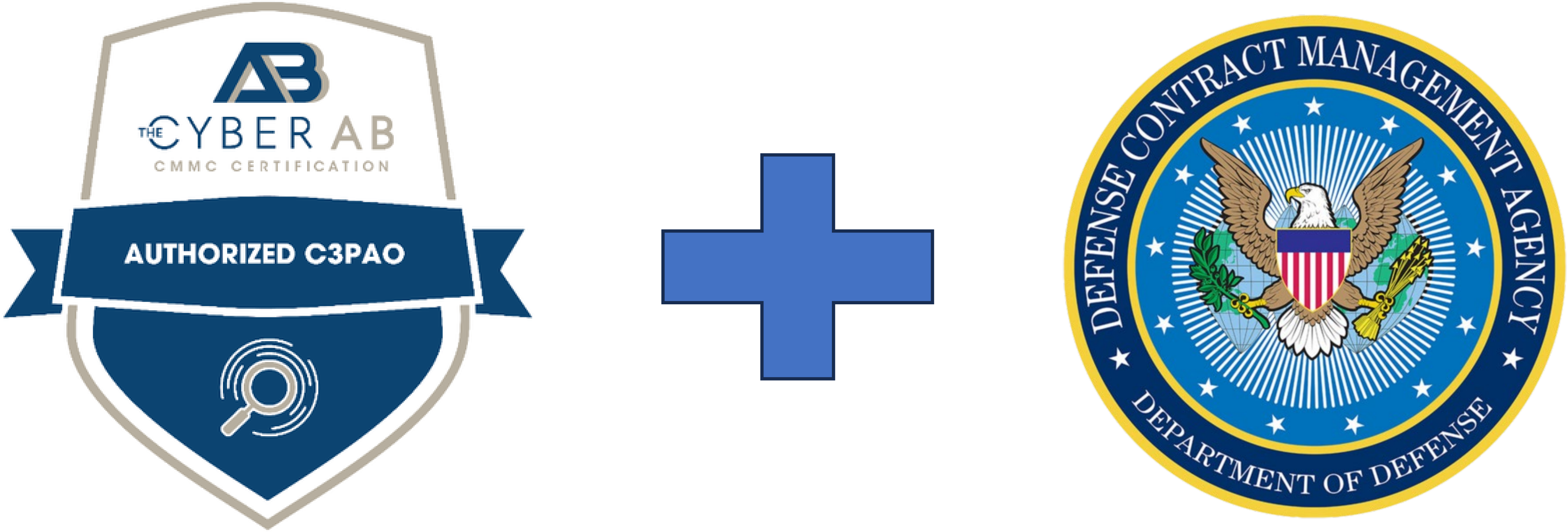
NIST SP 800-171A / CMMC ASSESSMENT PROCESS (CAP)

- Organizations [Certified Assessors] are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations [Certified Assessors] have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

NIST SP 800-171A / CMMC ASSESSMENT PROCESS (CAP)

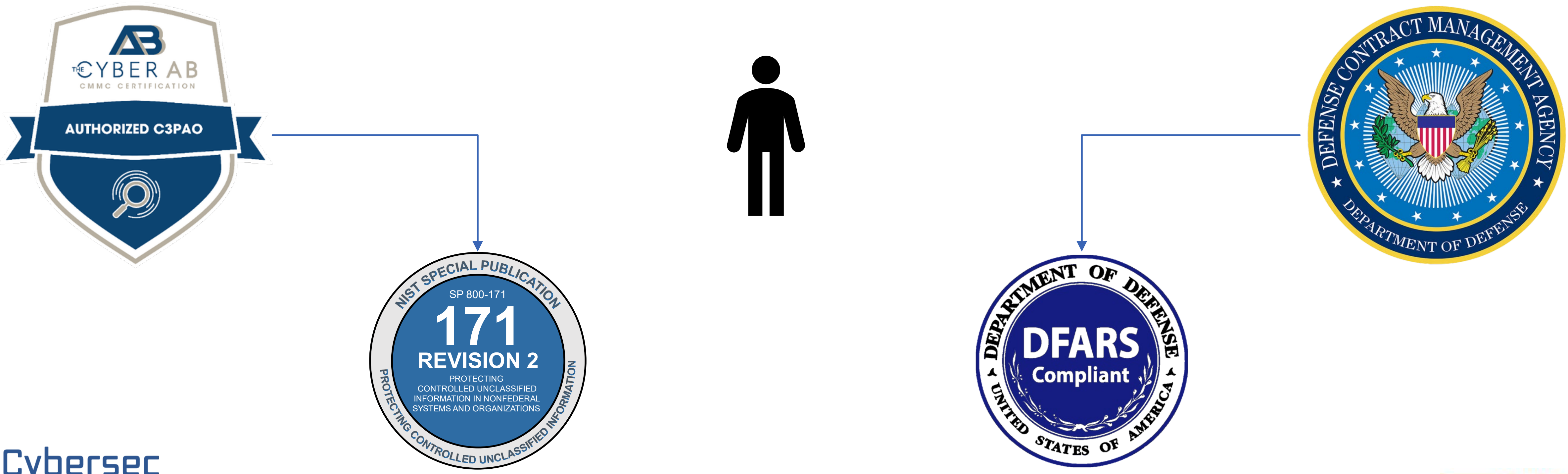
- Organizations [Certified Assessors] are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations [Certified Assessors] have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)



JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

DFARS 252.204-7012 Assessment



Cybersec
INVESTMENTS

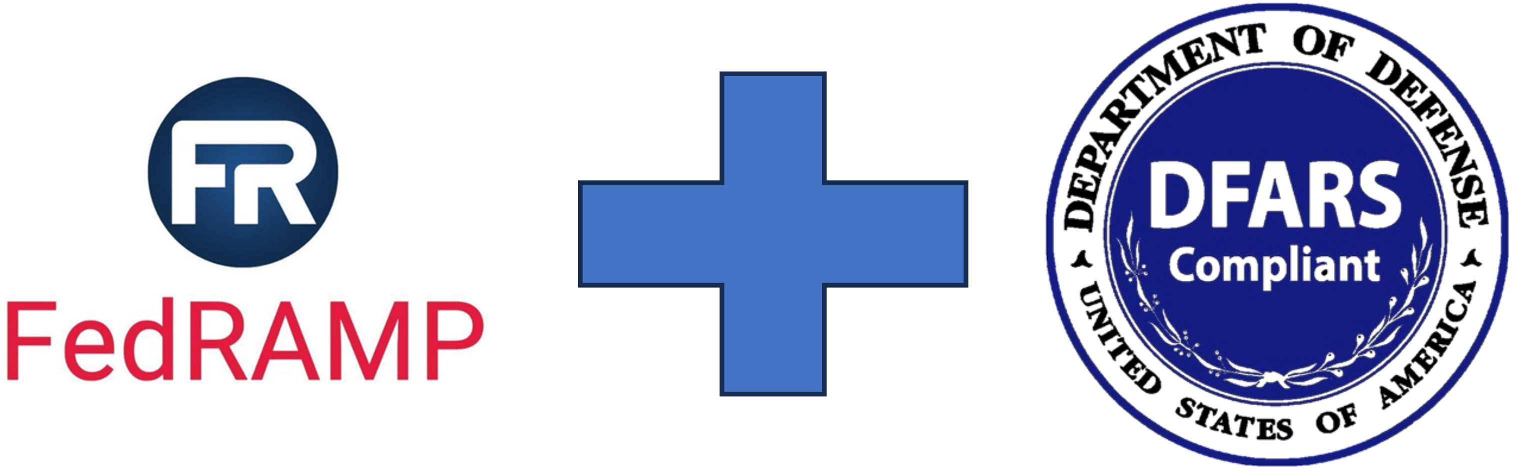
JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

- Medium-assurance certificate in accordance with paragraph (c)

IdenTrust™
part of HID Global

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

- Medium-assurance certificate in accordance with paragraph (c)
- Cloud service provider is FedRAMP Moderate or equivalent and complies with paragraphs (c) through (g)



JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

- Medium-assurance certificate in accordance with paragraph (c)
- Cloud service provider is FedRAMP Moderate or equivalent and complies with paragraphs (c) through (g)
- DFARS 252.204-7012 clause flow down in accordance with paragraph (m)

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

- “Our intent is if you go out and get a joint surveillance certification today, when the rule comes a thing and it’s real, then your certification will be good for another three years after that, provided you’ve made those annual affirmations and those annual affirmations are made by somebody in the C-suite…”

Stacy Bostjanick, Chief DIB Cybersecurity

PreVeil webinar

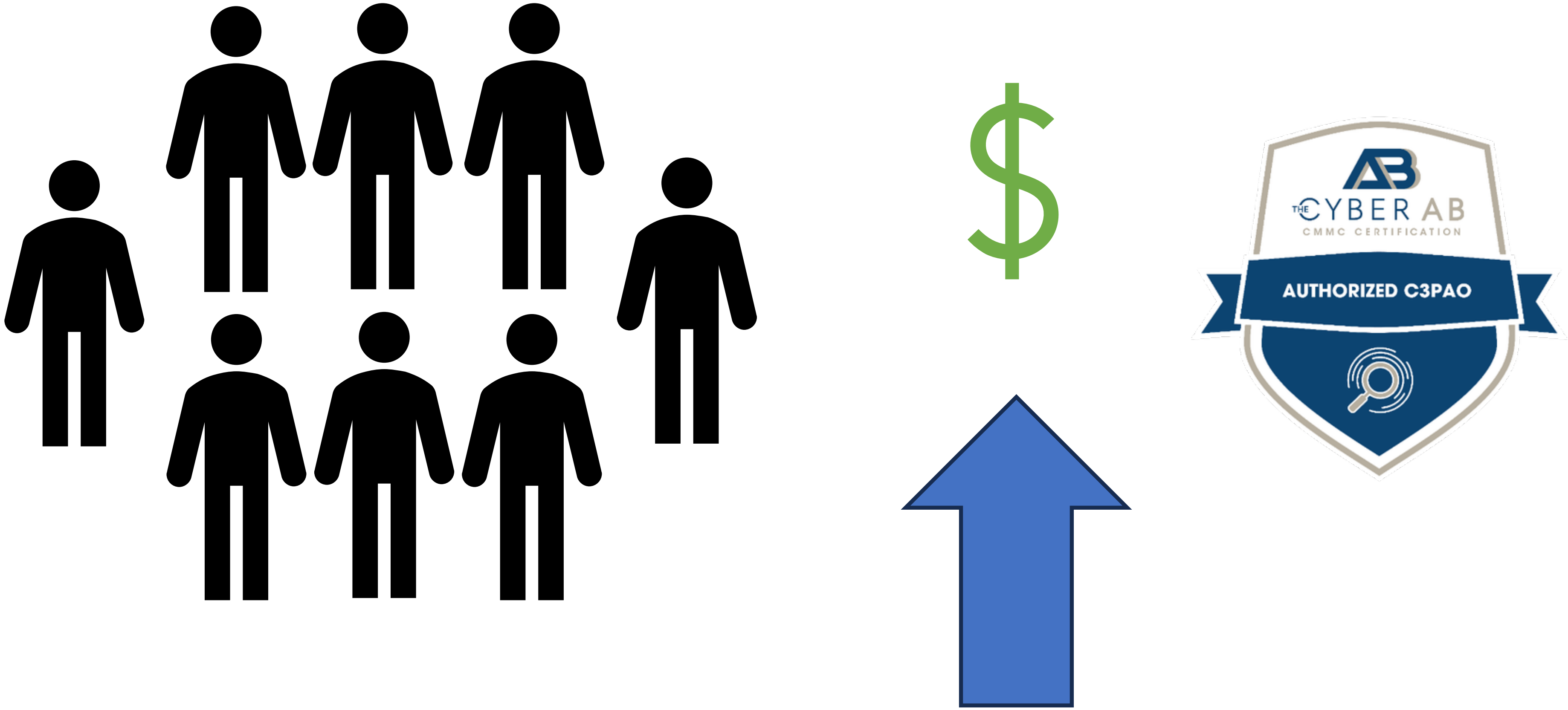
April 4, 2023

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO
$

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)

JOINT SURVEILLANCE VOLUNTARY ASSESSMENT (JSVA)



REFERENCES

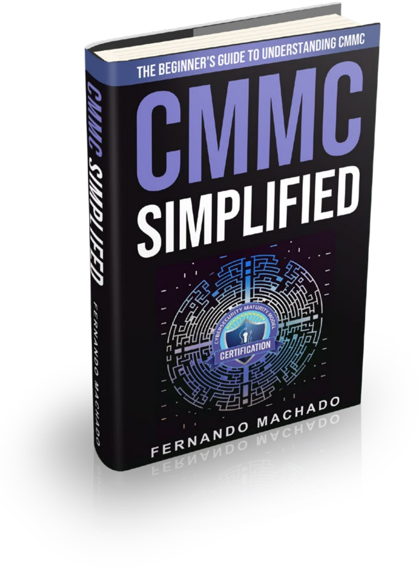
- *DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting*: https://www.acquisition.gov/dfars/252.204-7012cdic-ir-safeguarding-overed-efense-nformation-and-yberncident-eporting.
- *DFARS 252.204-7019*: https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.
- *DFARS 252.204-7020*: https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.
- *NIST SP 800-171 rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations:* https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- *NIST SP 800-171 rev. 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*: https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft
- *DoD Procurement Toolbox*: https://dodprocurementtoolbox.com/

QUESTIONS

FERNANDO MACHADO
CISO, CYBERSEC INVESTMENTS

- Services:
  - CMMC Advisory Services
  - CMMC Readiness Assessments
  - CMMC Level 2 Conformity Assessments
  - NIST SP 800-171 3rd Party Letter of Attestation

amazon



info@cybersecinvestments.com

1-800-960-8802

LinkedIn

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

CAICO
CERTIFIED CMMC ASSESSOR

CAICO
CERTIFIED CMMC PROFESSIONAL

Cybersec
INVESTMENTS

PUBLIC
Public Release Authorized