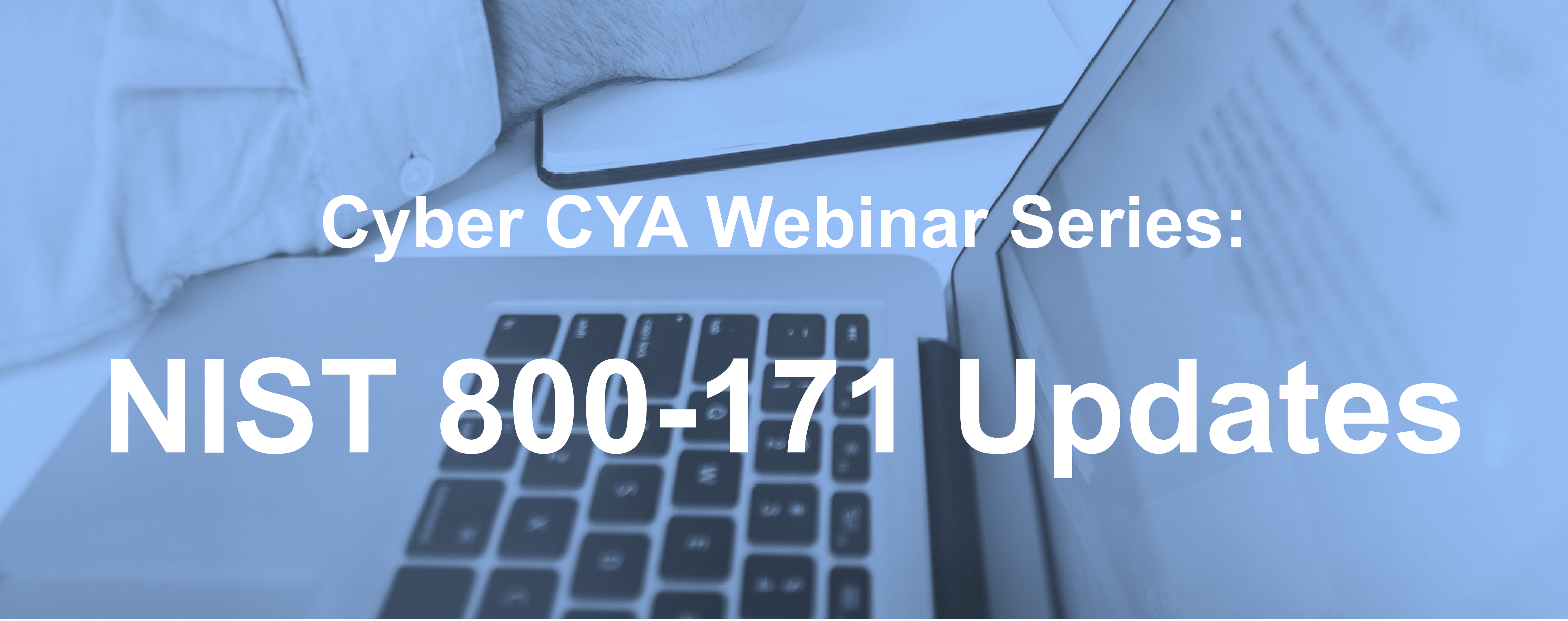


Cyber CYA Webinar Series:

NIST 800-171 Updates

Colorado SBDC

TECHSOURCE

CYBER: Cover Your Assets™

THE PIKES PEAK SMALL BUSINESS DEVELOPMENT CENTER HAS BEEN DEDICATED TO HELPING EXISTING AND NEW BUSINESSES GROW AND PROSPER FOR MORE THAN 30 YEARS.

FREE CONSULTING

PRACTICAL TRAINING

BUSINESS RESOURCES

Funded in part through a cooperative agreement with the U.S. Small Business Administration

WWW.PIKESPEAKSBDC.ORG/CONSULTING

WWW.PIKESPEAKSBDC.ORG/WORKSHOPS

Colorado SBDC
TECHSOURCE
CYBER: Cover Your Assets

Becoming DFARS / NIST Compliant

NIST SP 800-171 & Cybersecurity Maturity Model Certification – CMMC)

Dr. Shawn P. Murray, C|CISO, CISSP, CRISC

Revision: December 2019

Briefing Overview

- Content Structure

  - Define DFARS 252.204-7012
    - Controlled Defense Information
    - Contractor Internal System
    - Adequate Security Defined
  - Define NIST SP 800-171
    - Requirements Overview
    - Required Deliverables
    - Impact of non-compliance / teeth
  - Recommendations
    - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
    - Sample Recommendations
  - Conclusion

Intent

✓ Achieve understanding of the DFARS requirement

✓ Achieve understanding of how to achieve compliance with DFARS

✓ Identify industry "best practices" for becoming compliant

DFARS Clause 252.204-7012

- DFARS Clause 252.204-7012 requires contractors / sub-contractors to:

1. Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor’s internal information system or network
2. Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor’s ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. Submit media (if requested) and additional information to support a damage assessment
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.

Covered Defense Information – Definition

Covered defense information means:

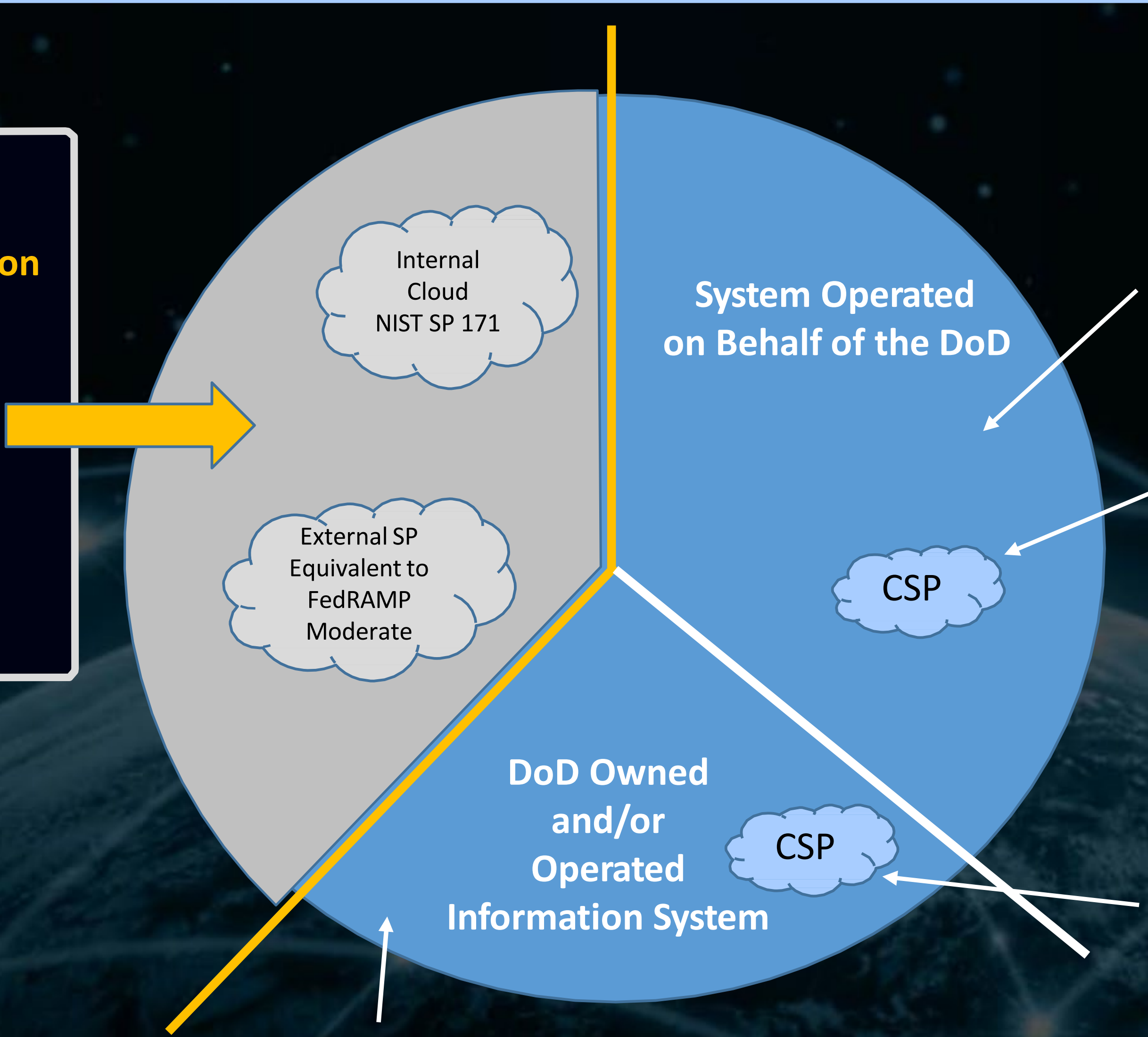
1. Unclassified controlled technical information (CTI) or other information as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with the law, regulations, and government-wide policies and is –
   a. Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR
   b. Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.*

* *In support of the performance of the contract is not meant to include the contractor's internal information (e.g., human resources or financial) that is incidental to the contract performance*

What Information Do You Need to Protect?

Contractor's Internal System

- Federal Contract Information
- Controlled Unclassified Information
- Covered Defense Information
  - Includes Unclassified Controlled Technical Information


Internal Cloud NIST SP 171
External SP Equivalent to FedRAMP Moderate
System Operated on Behalf of the DoD
CSP
DoD Owned and/or Operated Information System
CSP

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data o the DoD's behalf, DFARS clause 252.239-7010 and DoD Cloud Computing SRG apply

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG apply

Controlled Unclassified Information

Adequate Security Defined

- DFARS 252.204-7012 (b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:
  - (b)(2)(ii)(A): ***The Contractor shall implement NIST SP 800-171***, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017
  - Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

Briefing Overview

- Content Structure

- Define DFARS 252.204-7012
  - Controlled Defense Information
  - Contractor Internal System
  - Adequate Security Defined

- Define NIST SP 800-171
  - Requirements Overview
  - Required Deliverables
  - Impact of non-compliance / teeth

- Recommendations
  - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
  - Sample Recommendations

- Conclusion

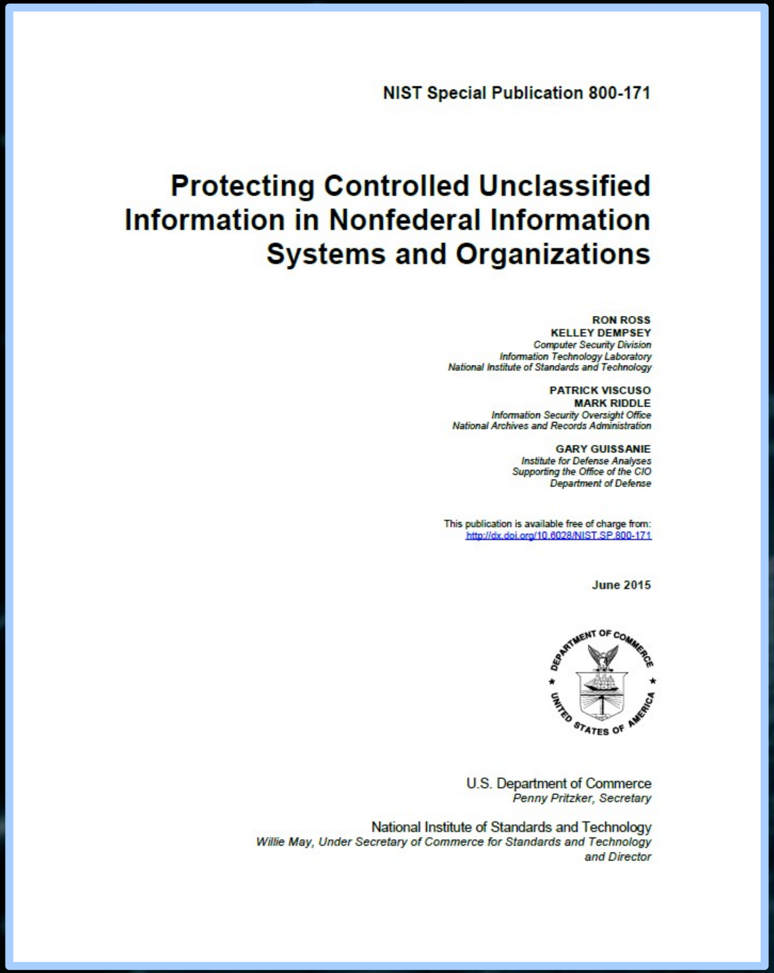
Intent

✓ Achieve understanding of the DFARS requirement

✓ Achieve understanding of how to achieve compliance with DFARS

✓ Identify industry “best practices” for becoming compliant

NIST SP 800-171 Requirements



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

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

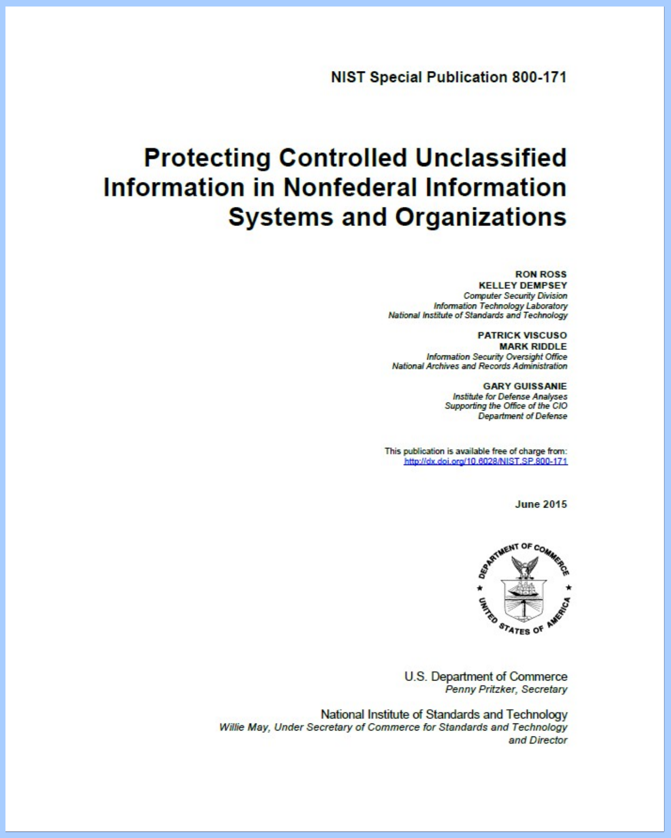
June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

- Details the security requirements to protect confidentiality of **Federal Contract Information, CDI, or CUI** on non-Federal information systems.
- Acts as a non-tailorable baseline, but offers flexibility in how to meet requirements
- Most requirements focus on policy, process, and configuring IT securely, but a number of controls may require security-related software or hardware.

NIST SP 800-171 Requirements



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

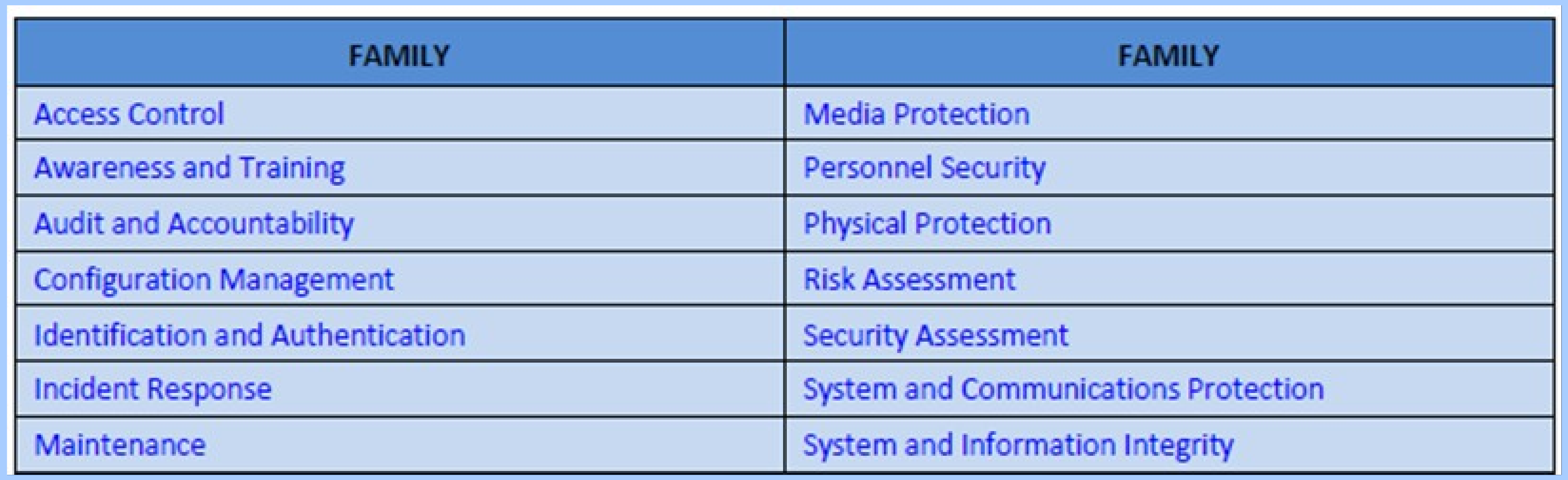
GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

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

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

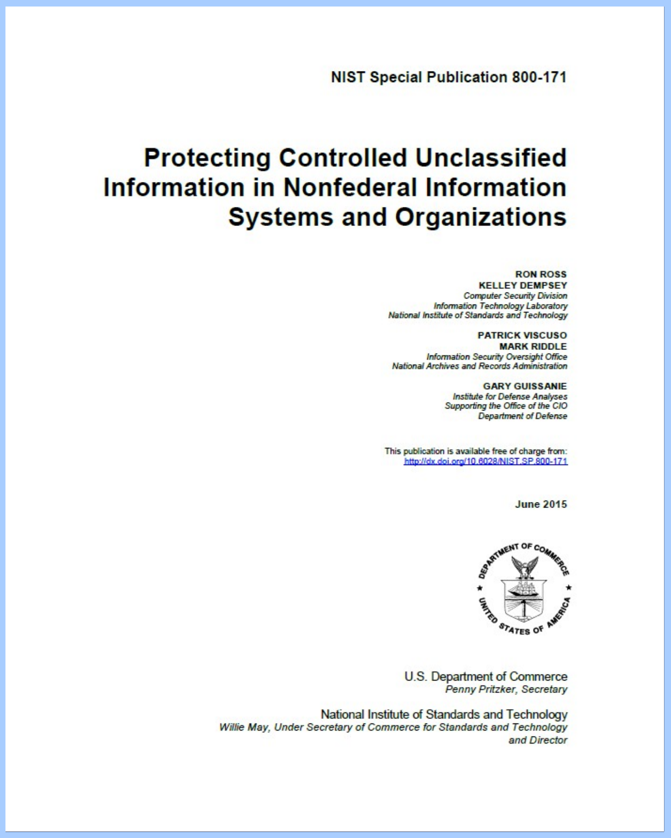
National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director



FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

- For ease of use, the security requirements are organized into 14 control families
- Each family contains the requirements related to the general security topic of the family, and contain a total of 110 individual controls/ requirements.

NIST SP 800-171 Required Deliverables



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

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

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

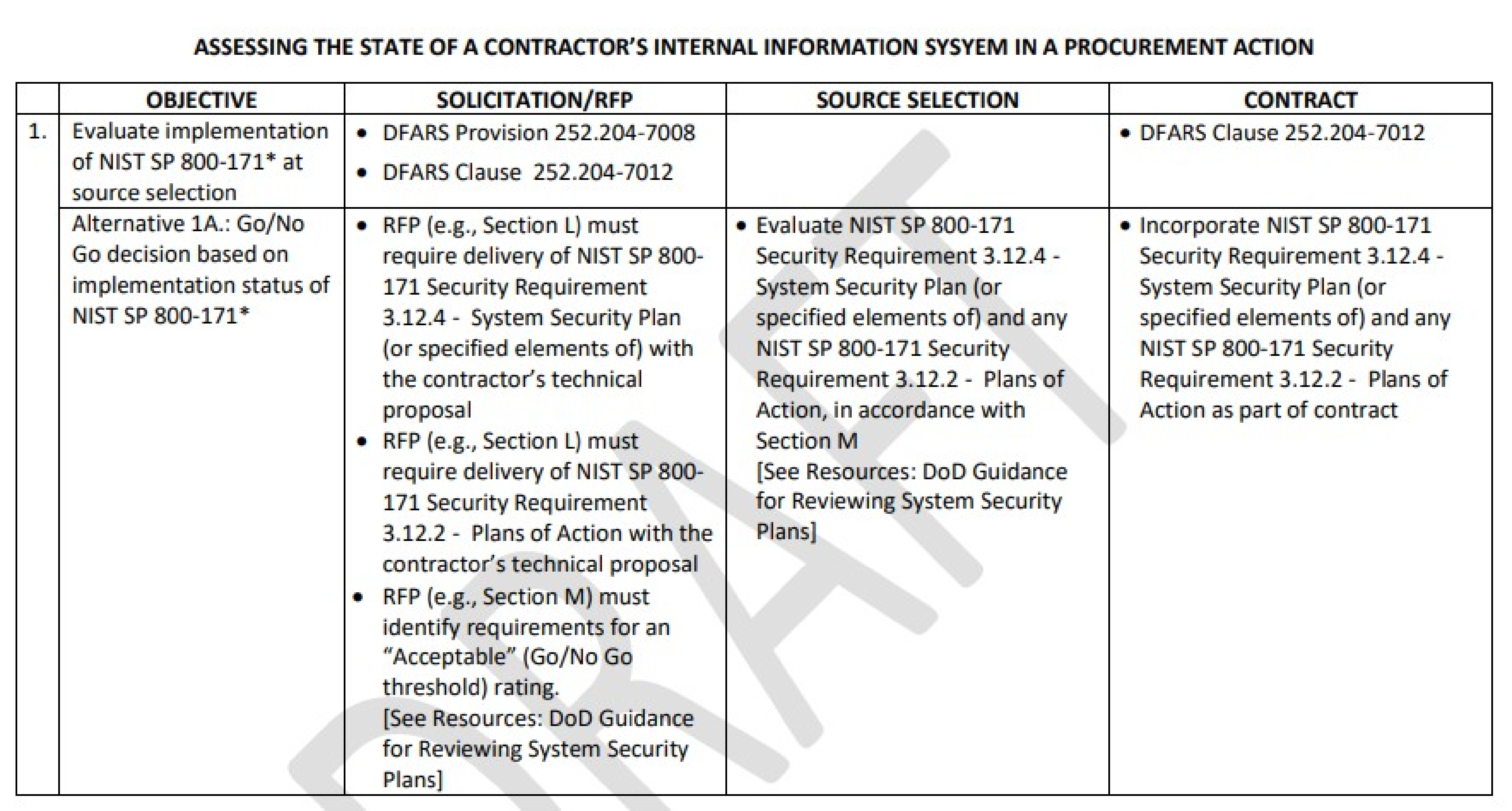
National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

To document implementation of NIST SP 800-171, companies should have a system security plan in place, in addition to any associated plans of action:

- NIST SP 800-171, Security Requirement 3.12.4 (System Security Plan):
  - 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
- NIST SP 800-171, Security Requirement 3.12.2 (Plans of Action):
  - Develop and implement ***plans of action*** designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

* *The contractor self-attests (by signing contract) to be compliant with DFARS Clause 252.204-7012, to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the system security plan and associated plans of action).*

NIST SP 800-171 Teeth



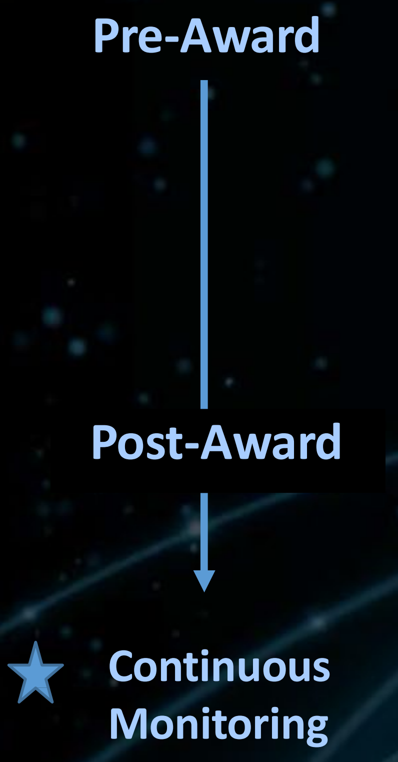
ASSESSING THE STATE OF A CONTRACTOR'S INTERNAL INFORMATION SYSYEM IN A PROCUREMENT ACTION

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
1.	Evaluate implementation of NIST SP 800-171* at source selection	• DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012		• DFARS Clause 252.204-7012
	Alternative 1A.: Go/No Go decision based on implementation status of NIST SP 800-171*	• RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) with the contractor's technical proposal • RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action with the contractor's technical proposal • RFP (e.g., Section M) must identify requirements for an "Acceptable" (Go/No Go threshold) rating. [See Resources: DoD Guidance for Reviewing System Security Plans]	• Evaluate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action, in accordance with Section M [See Resources: DoD Guidance for Reviewing System Security Plans]	• Incorporate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action as part of contract

- DARS-2018-0023-0002 "**Assessing the State of a Contractor's Internal Information System in a Procurement Action**" has been provided to illustrate how DoD may choose to assess submitted SSPs and POA&Ms in procurement actions that require the implementation of NIST SP 800-171.

https://www.regulations.gov/document?D=DARS-2018-0023-0002

NIST SP 800-171 Teeth



1. Evaluate implementation of NIST SP 800-171 at source selection
   - Alternative 1A: Go/No-Go Decision based on status of NIST SP 800-171 compliance
   - Alternative 1B: Assess NIST SP 800-171 implementation as a separate technical evaluation factor
2. Require protections in addition to the security requirements in NIST SP 800-171 and evaluate at source selection
3. Assess/Track implementation of NIST SP 800-171 security requirements after contract award
   - The government may also monitor compliance of NIST SP 800-171 (e.g. MDA CAT)
4. Contractors “self-attest” to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171

NOTE: In 2020 the DoD will require 3rd party certification under the Cybersecurity Maturity Model

- ✓ The Office of the Under Secretary of Defense for Acquisition is leading the effort.
- ✓ Currently CMMC Draft .7 is out for review

Office of the Under Secretary of Defense for Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Briefing Overview

- <u>Content Structure</u>

- Define DFARS 252.204-7012
  - Controlled Defense Information
  - Contractor Internal System
  - Adequate Security Defined

- Define NIST SP 800-171
  - Requirements Overview
  - Required Deliverables
  - Impact of non-compliance / teeth

- Recommendations
  - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
  - Sample Recommendations

- Conclusion

<u>Intent</u>

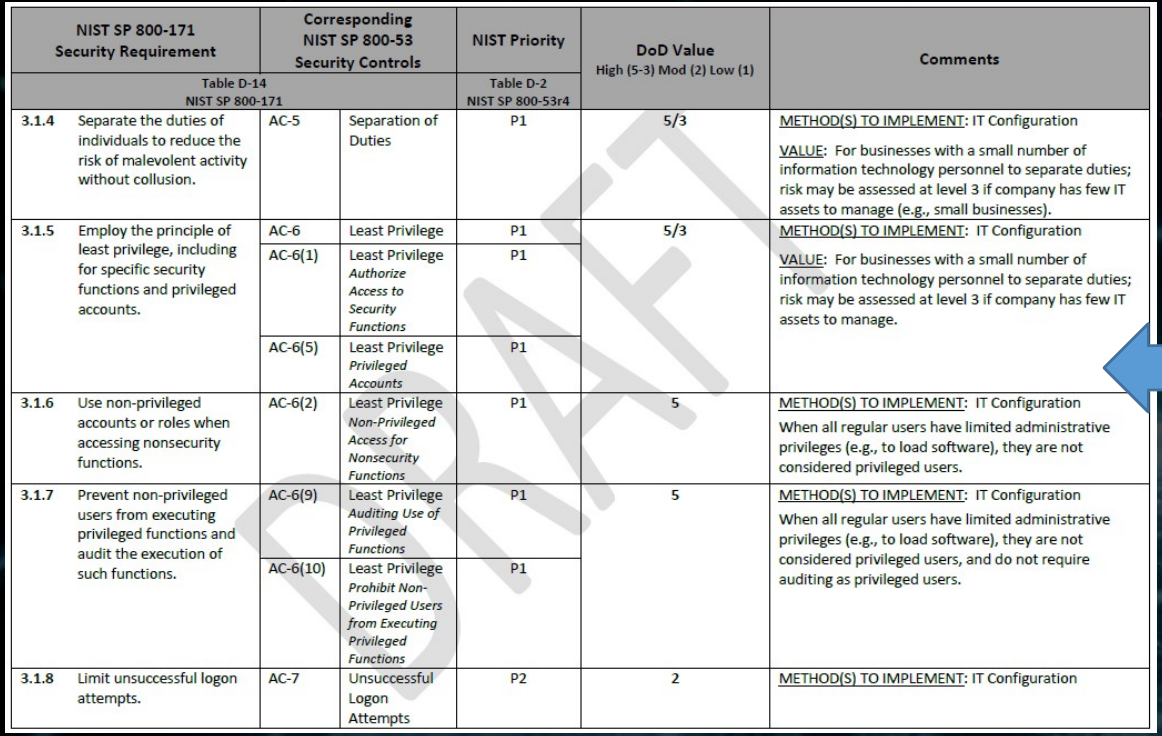
✓ Achieve understanding of the DFARS requirement

✓ Achieve understanding of how to achieve compliance with DFARS

✓ Identify industry "best practices" for becoming compliant

Recommendations

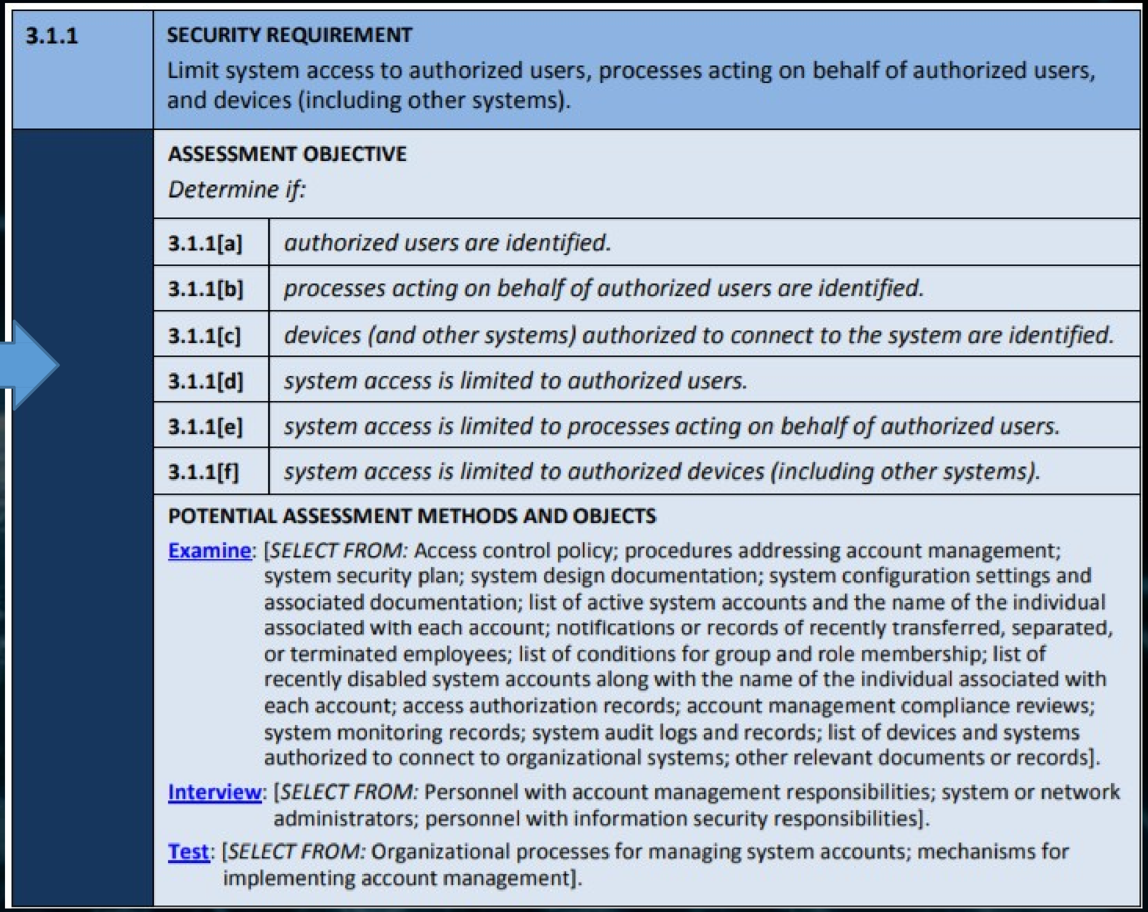
DoD Guidance for Reviewing SSPs and the NIST SP 800-171 Security Requirements Not Yet Implemented



NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	P1	5/3	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage (e.g., small businesses).
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	P1	5/3	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage.
		AC-6(1)	Least Privilege *Authorize Access to Security Functions*	P1		
		AC-6(5)	Least Privilege *Privileged Accounts*	P1		
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege *Non-Privileged Access for Nonsecurity Functions*	P1	5	METHOD(S) TO IMPLEMENT: IT Configuration When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	P1	5	METHOD(S) TO IMPLEMENT: IT Configuration When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users, and do not require auditing as privileged users.
		AC-6(10)	Least Privilege *Prohibit Non-Privileged Users from Executing Privileged Functions*	P1		
3.1.8	Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	P2	2	METHOD(S) TO IMPLEMENT: IT Configuration

- Two key artifacts should guide your efforts
- With limited time and resources, organizations may want to prioritize which controls to enact first as well as determine which controls may be implemented internally and which may require outside assistance.

NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*



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

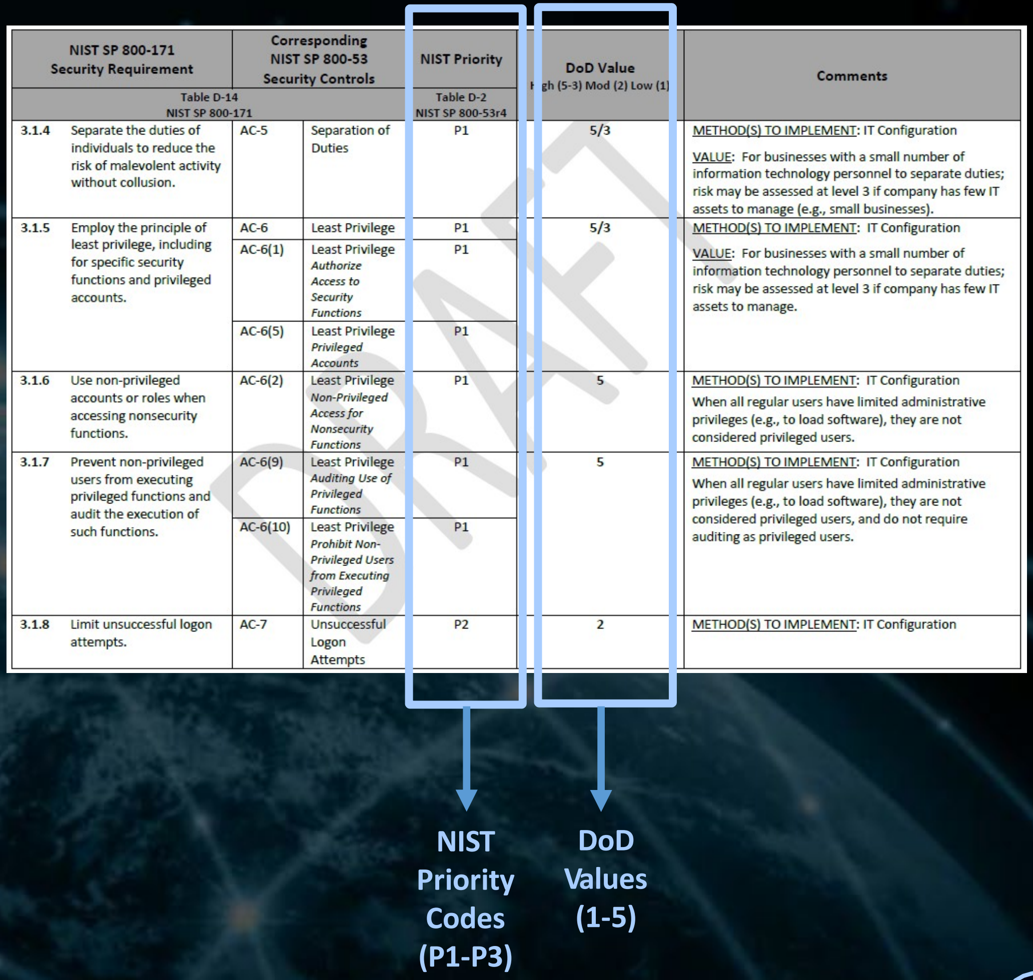
Recommendations

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

- "NIST SP 800-53 priority codes were considered in the calculation of the DoD Implementation Value for corresponding NIST SP 800-171 security requirements."
- "DoD Values range from 5 - representing the highest impact on the information system, or highest priority to implement, to 1 - representing the lowest impact on the information system, or lowest priority to implement."
- "The DoD Value for NIST SP 800-171 security requirements are typically 5, but may range between 5 and 3."

- **<u>"The guidance is not to be used to assess implemented security requirements, nor to compare or score a company's approach to implementing a security requirement."</u>**

https://www.regulations.gov/document?D=DARS-2018-0023-0002

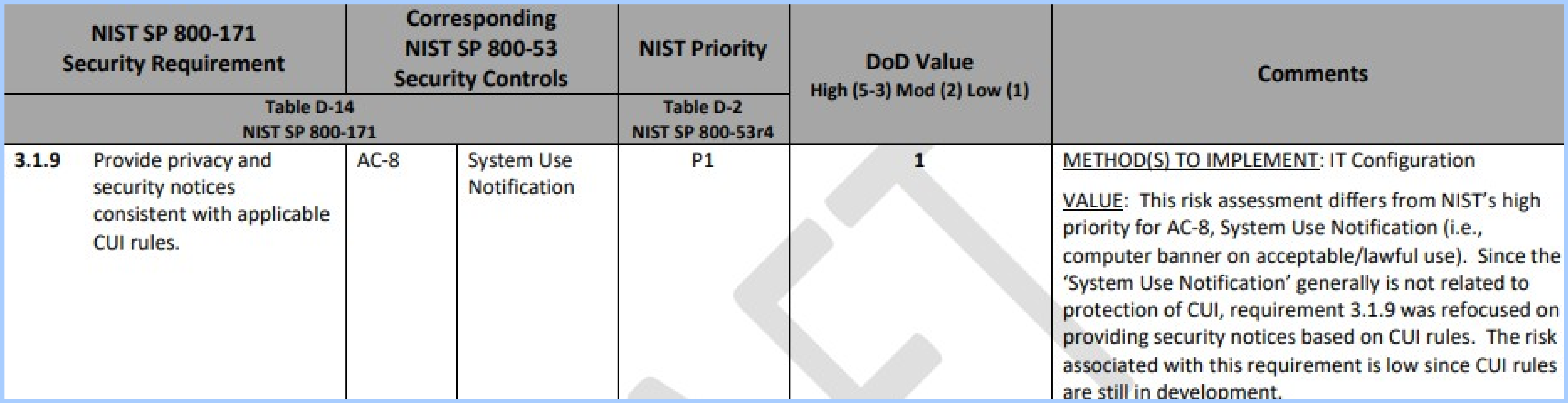


NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	P1	5/3	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration <u>VALUE</u>: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage (e.g., small businesses).
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	P1	5/3	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration <u>VALUE</u>: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage.
		AC-6(1)	Least Privilege *Authorize Access to Security Functions*	P1		
		AC-6(5)	Least Privilege *Privileged Accounts*	P1		
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege *Non-Privileged Access for Nonsecurity Functions*	P1	5	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	P1	5	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users, and do not require auditing as privileged users.
		AC-6(10)	Least Privilege *Prohibit Non-Privileged Users from Executing Privileged Functions*	P1		
3.1.8	Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	P2	2	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration

NIST Priority Codes (P1-P3)

DoD Values (1-5)

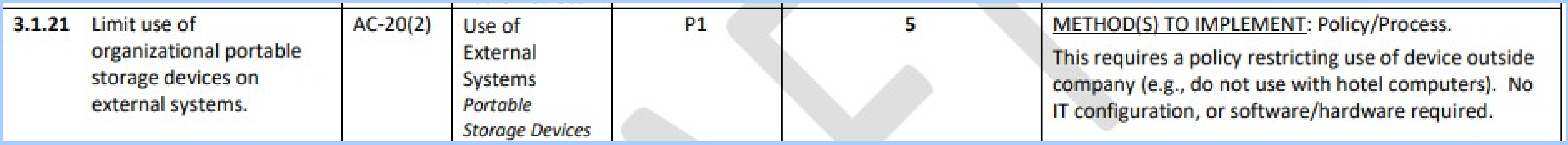
Sample Recommendation



NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	P1	**1**	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: This risk assessment differs from NIST's high priority for AC-8, System Use Notification (i.e., computer banner on acceptable/lawful use). Since the 'System Use Notification' generally is not related to protection of CUI, requirement 3.1.9 was refocused on providing security notices based on CUI rules. The risk associated with this requirement is low since CUI rules are still in development.

- "Where necessary, posters or other printed materials may be used in lieu of an automated system banner." NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.1.9, p71.

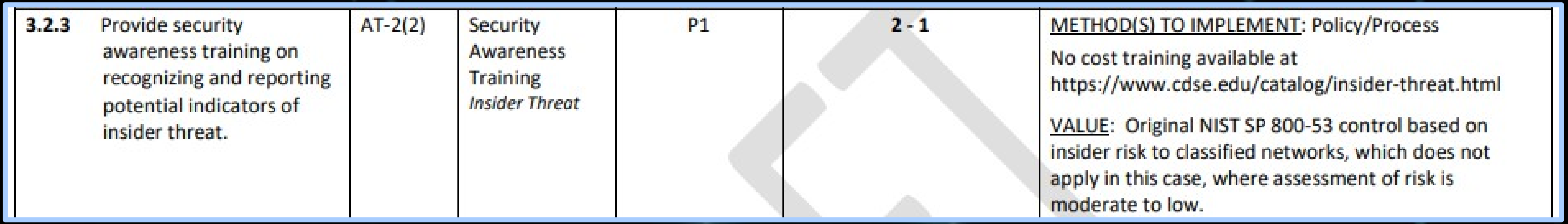
Sample Recommendation



3.1.21	Limit use of organizational portable storage devices on external systems.	AC-20(2)	Use of External Systems *Portable Storage Devices*	P1	**5**	<u>METHOD(S) TO IMPLEMENT</u>: Policy/Process. This requires a policy restricting use of device outside company (e.g., do not use with hotel computers). No IT configuration, or software/hardware required.

- "Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used." NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.1.21, p75.
- Even though this control is rated at a "5," the guidance shows that only a policy is required.
- Technical limitations/ configurations (e.g. Iron Key) are not required for this particular requirement.

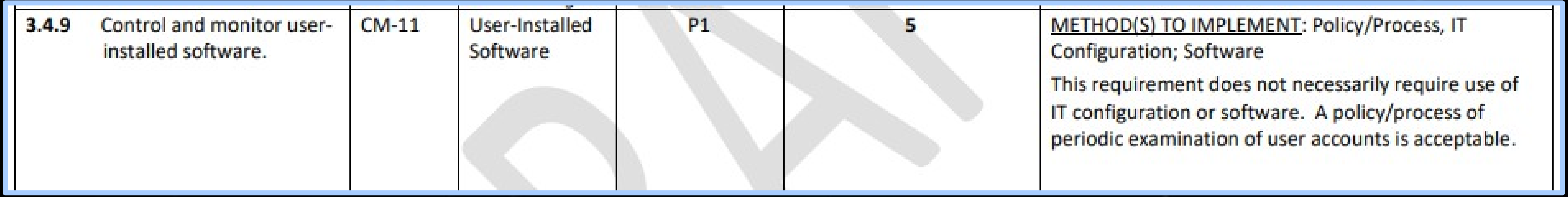
Sample Recommendation



3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	P1	**2 - 1**	METHOD(S) TO IMPLEMENT: Policy/Process No cost training available at https://www.cdse.edu/catalog/insider-threat.html VALUE: Original NIST SP 800-53 control based on insider risk to classified networks, which does not apply in this case, where assessment of risk is moderate to low.

- Free Basic Insider Threat Training: www.cdse.edu/catalog/elearning/INT101.html
- “Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations). NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.1.9, p76.
- Free In-Depth Insider Threat Training: www.cdse.edu/catalog/insider-threat.html

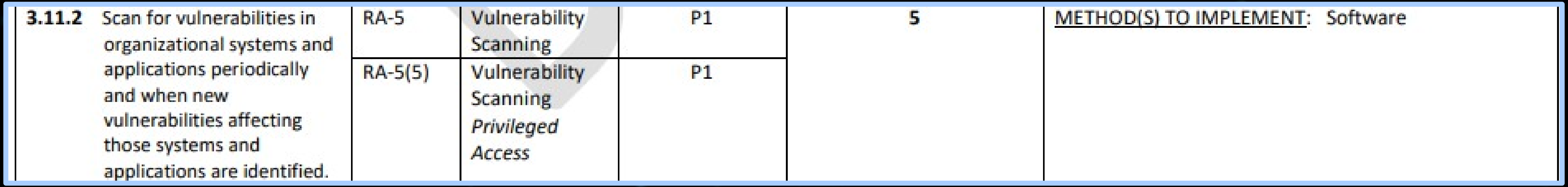
Sample Recommendation



3.4.9	Control and monitor user-installed software.	CM-11	User-Installed Software	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process, IT Configuration; Software This requirement does not necessarily require use of IT configuration or software. A policy/process of periodic examination of user accounts is acceptable.

- “Policy enforcement methods include procedural methods, automated methods, or both.” NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.4.9, p83.
- Even though this control is rated at a “5,” the guidance shows that only a policy is required.
- Information systems can be configured to automatically deny user-installed software, but this can be probative to organizations like software developers.

Sample Recommendation



3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	P1	**5**	<u>METHOD(S) TO IMPLEMENT</u>: Software
		RA-5(5)	Vulnerability Scanning *Privileged Access*	P1		

- "Vulnerability scanning includes, for example: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms." NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.11.2, p97.
- This control requires additional tools.
- The requirement may require outside assistance to define routine scan frequencies, configure scan utilities, and interpret scan results.
- Market is quickly evolving, and very cost effective and proven tools are now available (e.g., MARS Box)

Conclusion

- "DFARS Compliance" incorporates more than just following a simple DFARS clause
  - It encompasses protecting by implementing security controls established by NIST 800-171 and abiding by DFARS252.204-7012 in terms of protection and incident reporting

- There's a lot to do: Identifying **Federal Contract Information, CDI, or CUI** , determining which of the 110 NIST 800-171 Controls aren't in place in an SSP, planning for their remediation in a POA&M, and then actually implementing the controls

- All organizations have the opportunity to implement the requirements in-house, or they can contract out work to a third party to support a compliance assessment, policy development, architecture updates, or on-going monitoring.

- Depending on the complexity of your organization should drive this decision-making

- Talk to an SBDC Consultant.

Colorado SBDC
PIKES PEAK *Small Business Development Center*

Pikes Peak Small Business Development Center

559 E. Pikes Peak Ave., Suite 101, Colorado Springs, CO 80903

719-667-3803
sbdc@elpasoco.com

www.pikespeaksbdc.org

OUR SPONSORS:

EL PASO COUNTY COLORADO

COLORADO SPRINGS OLYMPIC CITY USA

connect 2DOT

COLORADO Office of Economic Development & International Trade Minority Business Office

Ent Business Banking

POWERED BY SBA U.S. Small Business Administration

Funded in part through a cooperative agreement with the U.S. Small Business Administration

Questions?

Reference Slides

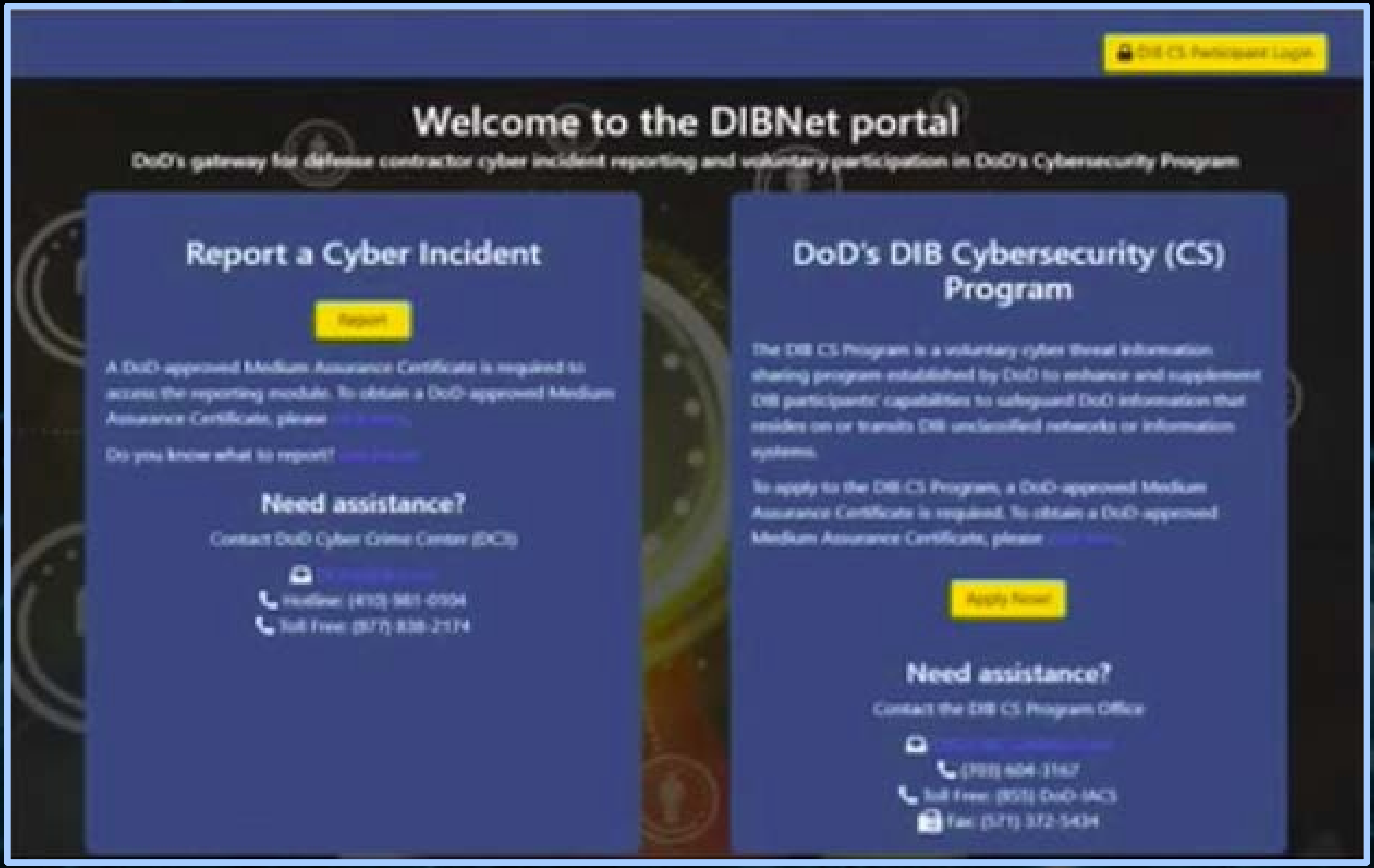
Cyber Incident Reporting

DFARS 204.7302 (d)

A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Contractors / sub-contractors must submit a cyber incident report via https://dibnet.dod.mil/
- Upon receipt of a cyber incident report –
  - DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s)
  - The contracting officer(s) provides the report to the requiring activities
  - DC3 analyzes report to identify cyber threat vectors and adversary trends
  - DCS contacts the reporting company if the report is incomplete

Cyber Incident Reporting



Welcome to the DIBNet portal

DoD's gateway for defense contractor cyber incident reporting and voluntary participation in DoD's Cybersecurity Program

Report a Cyber Incident

A DoD-approved Medium Assurance Certificate is required to access the reporting module. To obtain a DoD-approved Medium Assurance Certificate, please [illegible]

Do you know what to report? [illegible]

Need assistance?

Contact DoD Cyber Crime Center (DC3)

[illegible]
Hotline: (410) 981-0104
Toll Free: (877) 838-2174

DoD's DIB Cybersecurity (CS) Program

The DIB CS Program is a voluntary cyber threat information sharing program established by DoD to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems.

To apply to the DIB CS Program, a DoD-approved Medium Assurance Certificate is required. To obtain a DoD-approved Medium Assurance Certificate, please [illegible]

Need assistance?

Contact the DIB CS Program Office

[illegible]
(703) 604-3167
Toll Free: (855) DoD-IACS
Fax: (571) 372-5434

Sub-Contractor Flow down

When should DFARS clause 252.204-7012 flow down to sub-contractors?

- The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information
- The contractor shall determine if the information required for subcontractor performance is, or retains its identity as, covered defense information and requires safeguarding
- Flow down is a requirement of the terms of the contract with the government, which must be enforced by the prime contractor as a result of compliance with these terms
  - If a sub-contractor does not agree to comply with the terms of DFARS clause 252.204-7012, then covered defense information shall not be shared with the sub-contractor or otherwise reside on its information system

The DoD's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flow down of information requiring protection

Resources

- Jamie Miller, President & CEO – original presentation in August 2018
  - https://business.defense.gov/Portals/57/Documents/BPIIMPTW18%20slides/becoming%20dfars%20nist%20compliant.pdf?ver=2018-08-21-194207-740
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information
  - This document is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in SP 800-171, *Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations*
  - Becoming DFARS / NIST Compliant
  - *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf*
- Cybersecurity Evaluation Tool (CSET)
  - No-cost application, developed by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control systems and IT network security practices
  - *https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET*
- NIST MEP Handbook Cybersecurity Handbook (HB-162)
  - Handbook provides a step-by-step guide to assessing a small manufacturer's information systems against the security requirements in NIST SP 800-171, rev 1 ,"*Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations*"
  - *https://www.nist.gov/mep*

Colorado SBDC
PIKES PEAK *Small Business Development Center*

Pikes Peak Small Business Development Center

559 E. Pikes Peak Ave., Suite 101, Colorado Springs, CO 80903

719-667-3803
sbdc@elpasoco.com

www.pikespeaksbdc.org

OUR SPONSORS:

El Paso County Colorado

Ent Business Banking

Colorado Springs Olympic City USA

PSBTrust.com Park State Bank & Trust

CenturyLink

VectraBank Colorado

Powered by SBA U.S. Small Business Administration

Funded in part through a cooperative agreement with the U.S. Small Business Administration