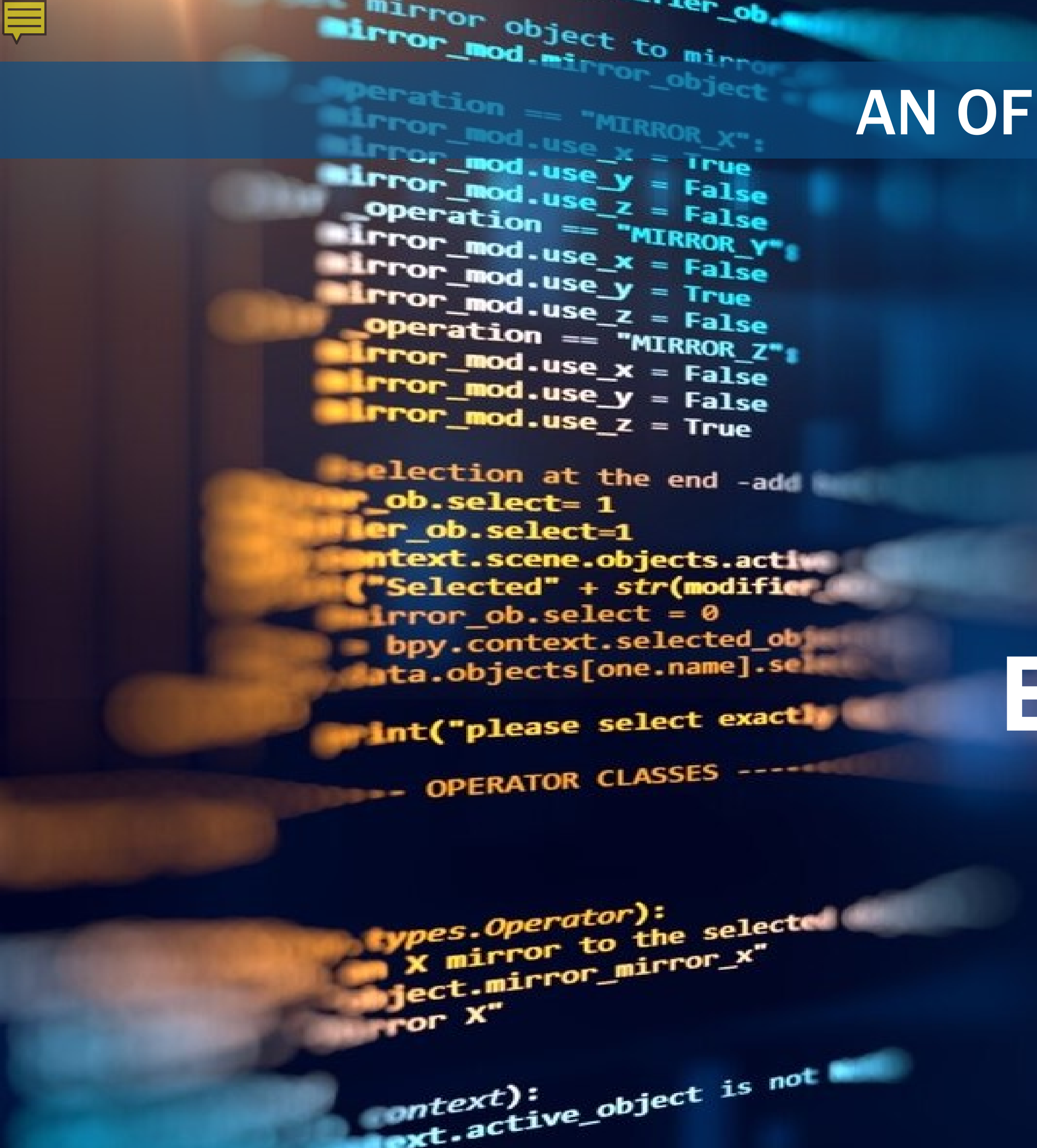


AN OFFERING IN THE BLUE CYBER SERIES:

CMMC Level 1 And FAR 52.204-21: Basic Cyber Hygiene

Version 14 Mar 2022

#16 in the Blue Cyber Education Series

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2022-0373, 27 Jan 2022

NIST 800-171 SECURITY REQUIREMENTS

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
🟦 3.1.1	🟧 3.2.1	🟦 3.3.1	🟢 3.4.1	🟦 3.5.1	🟧 3.6.1	🟨 3.7.1	🟧 3.8.1	🟧 3.9.1	🟧 3.10.1	🟢 3.11.1	🟢 3.12.1	🟪 3.13.1	🟧 3.14.1
🟦 3.1.2	🟧 3.2.2	🟦 3.3.2	🟥 3.4.2	🟦 3.5.2	🟢 3.6.2	⬛ 3.7.2	🟧 3.8.2	🟧 3.9.2	🟧 3.10.2	🟩 3.11.2	⬛ 3.12.2	🟢 3.13.2	🟩 3.14.2
🟧 3.1.3	🟧 3.2.3	🟢 3.3.3	🟧 3.4.3	⬜ 3.5.3	🟢 3.6.3	⬛ 3.7.3	🟫 3.8.3		🟧 3.10.3	⬛ 3.11.3	⬛ 3.12.3	🟦 3.13.3	🟢 3.14.3
🟦 3.1.4		🟦 3.3.4	🟢 3.4.4	🟫 3.5.4		🟨 3.7.4	🟧 3.8.4		🟧 3.10.4		⬛ 3.12.4	🟫 3.13.4	🟦 3.14.4
🟦 3.1.5		🟢 3.3.5	🟧 3.4.5	🟦 3.5.5		🟫 3.7.5	🟧 3.8.5		🟧 3.10.5			🟦 3.13.5	🟩 3.14.5
🟧 3.1.6		🟩 3.3.6	🟦 3.4.6	🟦 3.5.6		⬛ 3.7.6	🟥 3.8.6		🟧 3.10.6			🟦 3.13.6	⬜ 3.14.6
🟦 3.1.7		🟦 3.3.7	🟥 3.4.7	🟦 3.5.7			🟥 3.8.7					🟦 3.13.7	🟩 3.14.7
🟦 3.1.8		🟦 3.3.8	🟥 3.4.8	🟦 3.5.8			🟧 3.8.8					🟫 3.13.8	
🟧 3.1.9		🟦 3.3.9	🟥 3.4.9	🟦 3.5.9			🟫 3.8.9					🟦 3.13.9	
🟦 3.1.10				🟦 3.5.10								🟫 3.13.10	
🟦 3.1.11				🟦 3.5.11								🟫 3.13.11	
🟢 3.1.12												🟦 3.13.12	
🟩 3.1.13												🟫 3.13.13	
🟪 3.1.14												🟫 3.13.14	
🟦 3.1.15												🟦 3.13.15	
🟦 3.1.16												🟥 3.13.16	
🟦 3.1.17													
🟦 3.1.18													
🟩 3.1.19													
🟢 3.1.20													
🟧 3.1.21													
🟧 3.1.22													

🟧	Administrative (e.g., policies, standards & procedures)	🟢	Assigned Tasks To Cybersecurity Personnel
🟦	Technical Configurations (e.g., security settings)	🟨	Assigned Tasks To IT Personnel
🟩	Software Solution	⬛	Assigned Tasks To Application/ Asset/Process Owner
🟪	Hardware Solution	🟥	Configuration or Software Solution
⬜	Software or Hardware Solution	🟫	Configuration or Software or Hardware or Outsourced Solution

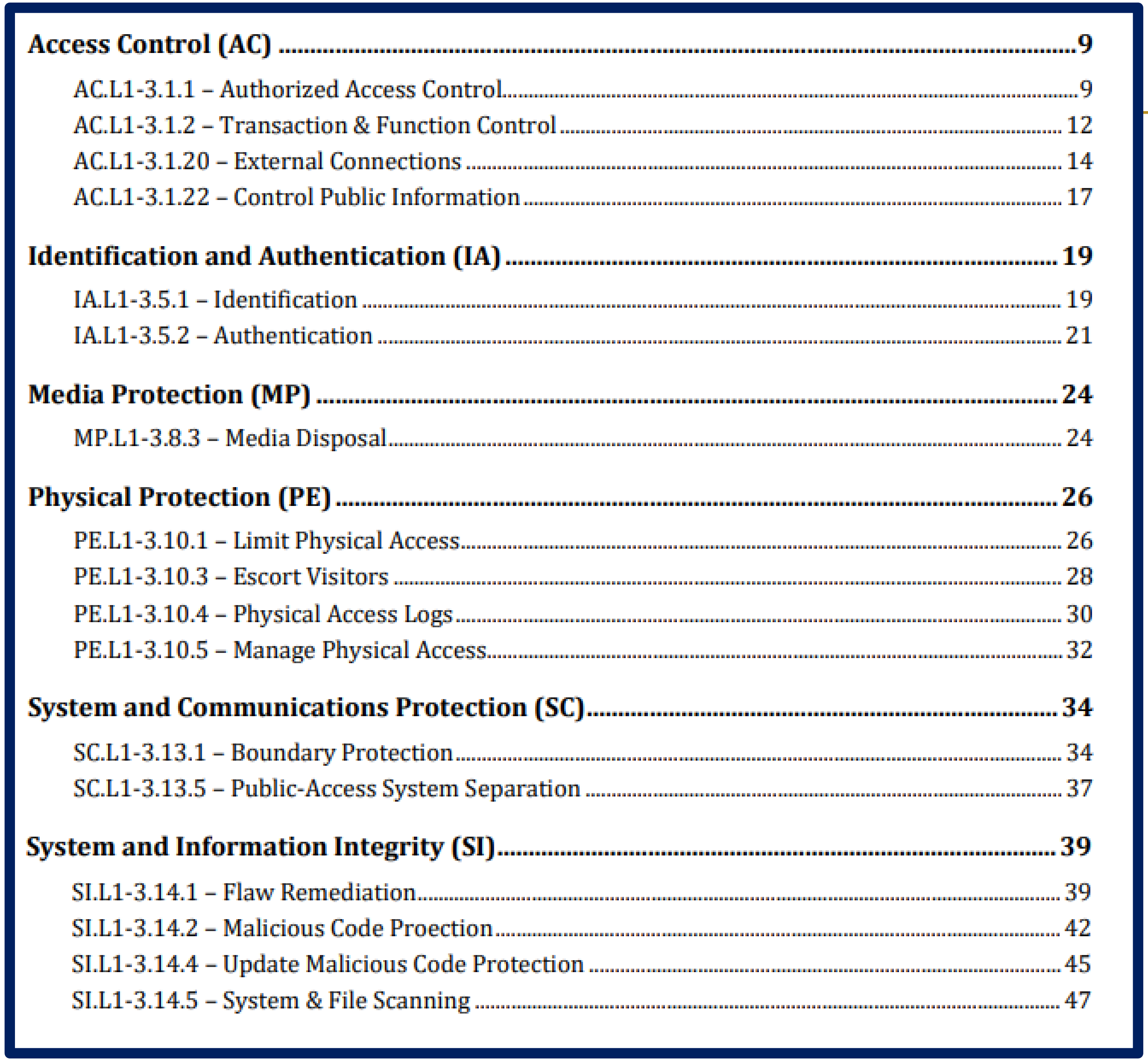
NIST 800-171 SECURITY REQUIREMENTS

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1				3.5.1					3.10.1			3.13.1	3.14.1
3.1.2				3.5.2									3.14.2
							3.8.3		3.10.3				
									3.10.4				3.14.4
3.1.20									3.10.5			3.13.5	3.14.5
3.1.22													

17 NIST SP 800-171 Security Requirements are the same as:
CMMC 2.0 Level 1 Security Requirements and the same as
FAR 52.204-21 Security Requirements

Same/Same/Same

17 Controls to Assess and Document



FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(i)	3.1.1 Technical Control	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
(b)(1)(ii)	3.1.2 Technical Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(b)(1)(iii)	3.1.20 Technical Control Administrative Control	Verify and control/limit connections to and use of external information systems.
(b)(1)(iv)	3.1.22 Administrative Control	Control information posted or processed on publicly accessible information systems.
(b)(1)(v)	3.5.1 Technical Control	Identify information system users, processes acting on behalf of users or devices.

Laundry List of Artifacts which are meant to give you ideas of what kind of Objective Proof you can supply on each of the 110 requirements

- Documented policies, standards & procedures
- Supporting documentation to demonstrate how (software, hardware, etc.) is properly & securely implemented
- Screen shot of everything that could provide objective proof
- Documents or screenshot which demonstrate a capability
- Documents or screenshot to show how software or hardware are properly and securely configured
- Screen Shots groups and membership assignment
- Documentation to demonstrate change management practices reviewed/approved
- Data Flow Diagram (DFD)
- Screen shot of firewall rules with business justification
- Documentation of role-based security training being performed
- Screen shot of access control settings
- Screen shot of AD settings, or other IAM interface

** One solution, could be others.*

FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(vi)	3.5.2 Technical Control	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.
(b)(1)(vii)	3.8.3 Configuration or Software or Hardware or Outsource	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.
(b)(1)(viii)	3.10.1 Administrative Control	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.
(b)(1)(ix)	3.10.3 Administrative Control	Escort visitors and monitor visitor activity.
(b)(1)(ix)	3.10.4 Administrative Control	Maintain audit logs of physical access.

Laundry List of Artifacts which are meant to give you ideas of what kind of Objective Proof you can supply on each of the 110 requirements

- Documented policies, standards & procedures
- Supporting documentation to demonstrate how (software, hardware, etc.) is properly & securely implemented
- Screen shot of everything that could provide objective proof
- Documents or screenshot which demonstrate a capability
- Documents or screenshot to show how software or hardware are properly and securely configured
- Screen Shots groups and membership assignment
- Documentation to demonstrate change management practices reviewed/approved
- Data Flow Diagram (DFD)
- Screen shot of firewall rules with business justification
- Documentation of role-based security training being performed
- Screen shot of access control settings
- Screen shot of AD settings, or other IAM interface

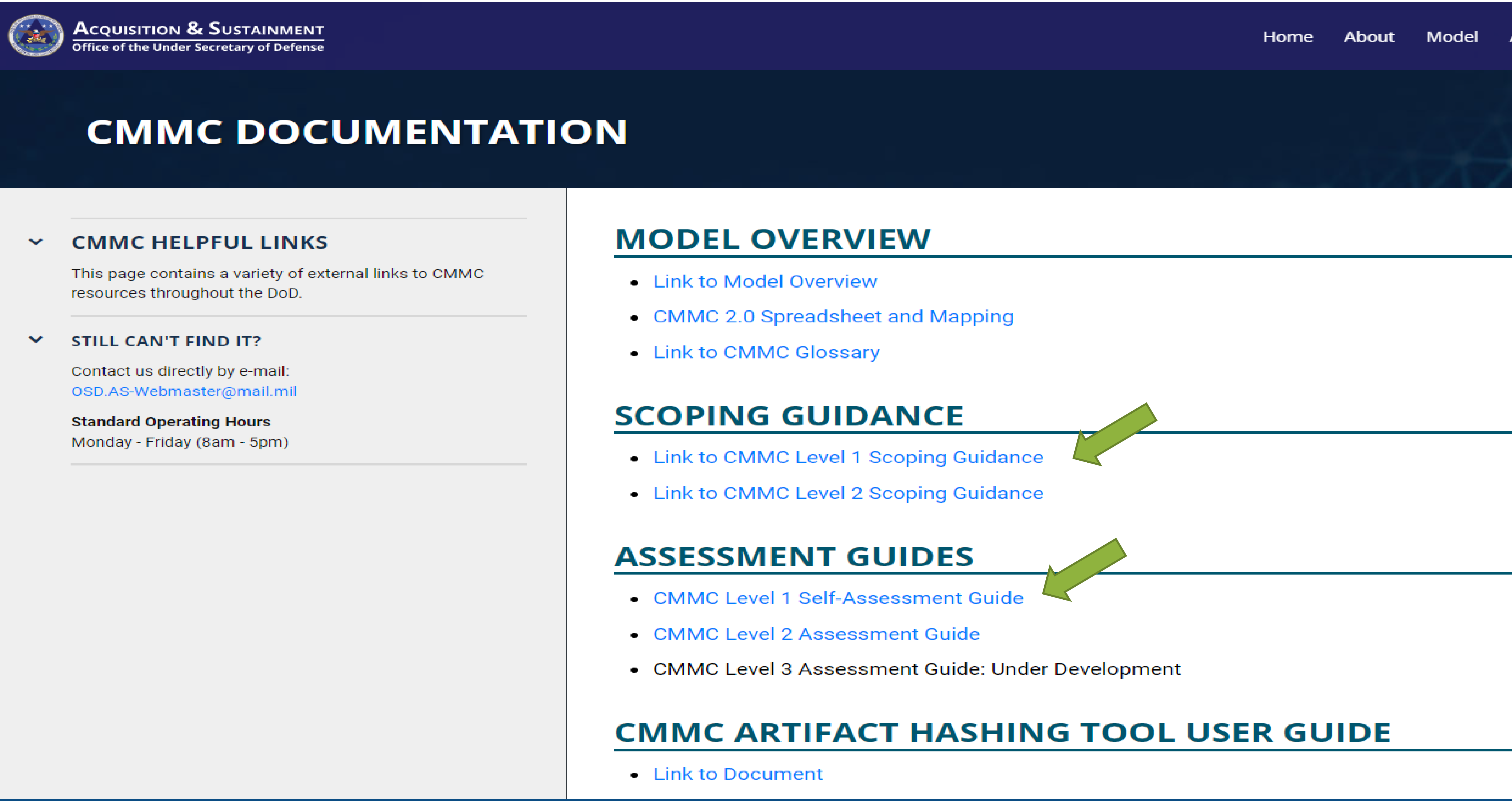
** One solution, could be others.*

FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(ix)	3.10.5 Administrative Control Physical Control	Control and manage physical access devices.
(b)(1)(x)	3.13.1 Hardware Solution*	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(b)(1)(xi)	3.13.5 Technical Control	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(b)(1)(xii)	3.14.1 Administrative Control	Identify, report and correct information and information system flaws in a timely manner.
(b)(1)(xiii)	3.14.2 Software Solution*	Provide protection from malicious code at appropriate locations within organizational information systems.
(b)(1)(xiv)	3.14.4 Technical Control	Update malicious code protection mechanisms when new releases are available.
(b)(1)(xv)	3.14.5 Software Solution*	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.

Laundry List of Artifacts which are meant to give you ideas of what kind of Objective Proof you can supply on each of the 110 requirements

- Documented policies, standards & procedures
- Supporting documentation to demonstrate how (software, hardware, etc.) is properly & securely implemented
- Screen shot of everything that could provide objective proof
- Documents or screenshot which demonstrate a capability
- Documents or screenshot to show how software or hardware are properly and securely configured
- Screen Shots groups and membership assignment
- Documentation to demonstrate change management practices reviewed/approved
- Data Flow Diagram (DFD)
- Screen shot of firewall rules with business justification
- Documentation of role-based security training being performed
- Screen shot of access control settings
- Screen shot of AD settings, or other IAM interface

** One solution, could be others.*



Acquisition & Sustainment
Office of the Under Secretary of Defense
Home
About
Model

CMMC DOCUMENTATION

CMMC HELPFUL LINKS

This page contains a variety of external links to CMMC resources throughout the DoD.

STILL CAN'T FIND IT?

Contact us directly by e-mail:
OSD.AS-Webmaster@mail.mil

Standard Operating Hours
Monday - Friday (8am - 5pm)

MODEL OVERVIEW

- Link to Model Overview
- CMMC 2.0 Spreadsheet and Mapping
- Link to CMMC Glossary

SCOPING GUIDANCE

- Link to CMMC Level 1 Scoping Guidance
- Link to CMMC Level 2 Scoping Guidance

ASSESSMENT GUIDES

- CMMC Level 1 Self-Assessment Guide
- CMMC Level 2 Assessment Guide
- CMMC Level 3 Assessment Guide: Under Development

CMMC ARTIFACT HASHING TOOL USER GUIDE

- Link to Document

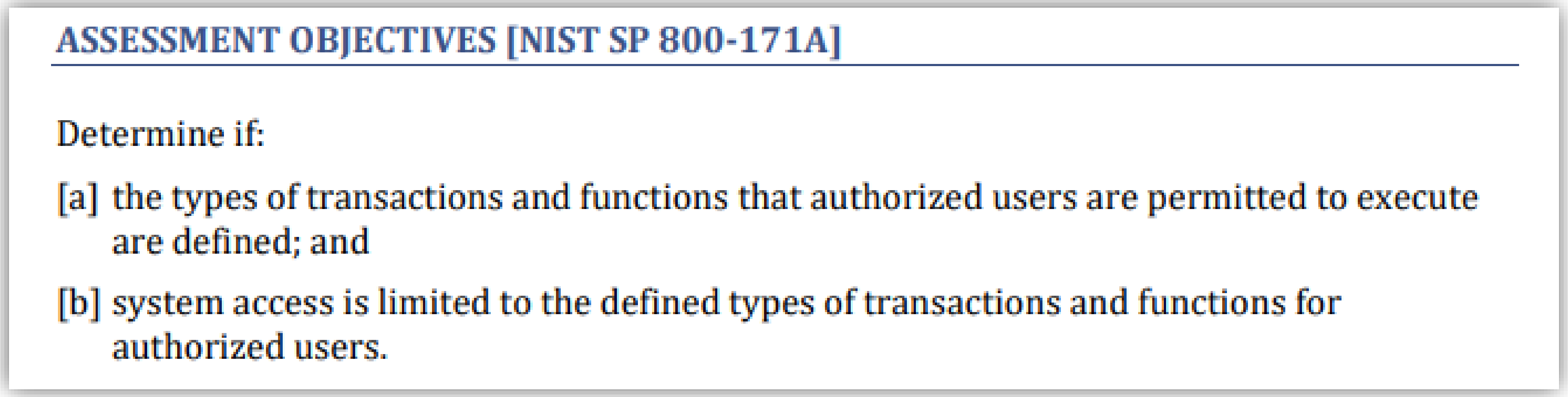
Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2022-0373, 27 Jan 2022

How to use these CMMC 2.0 Documents

- Inventory your Information System
  - See the Blue Cyber "Where to begin with NIST SP 800-171"
- Scope your Assessment
- Utilize the Key Sections of the Self-Assessment Guide
  1. Assessment Objectives from NIST SP 800-171A
  2. Potential Assessment Methods
  3. Discussion (provides a practical understanding)
  4. Further Discussion
  5. Example
  6. Potential Assessment Considerations

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.



ASSESSMENT OBJECTIVES [NIST SP 800-171A]

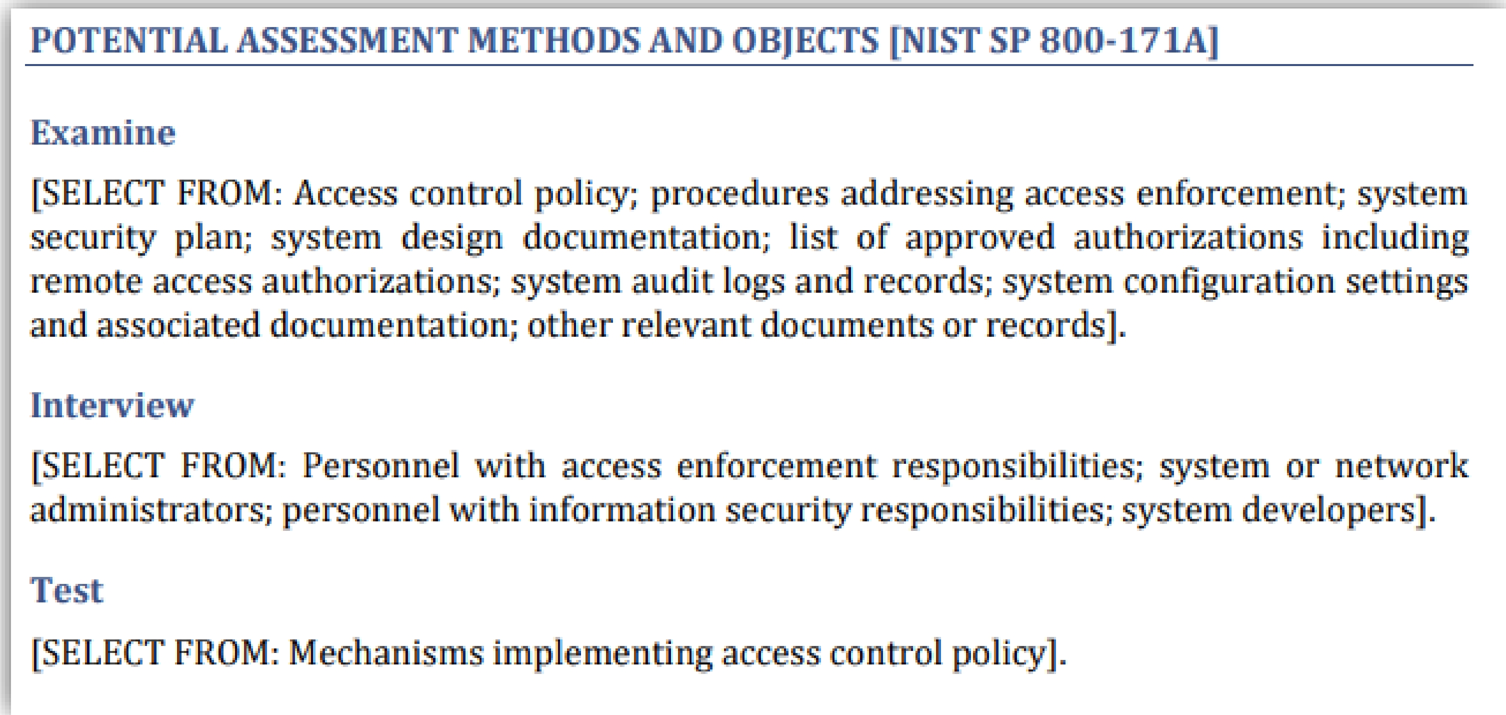
Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[b] system access is limited to the defined types of transactions and functions for authorized users.

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.



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

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

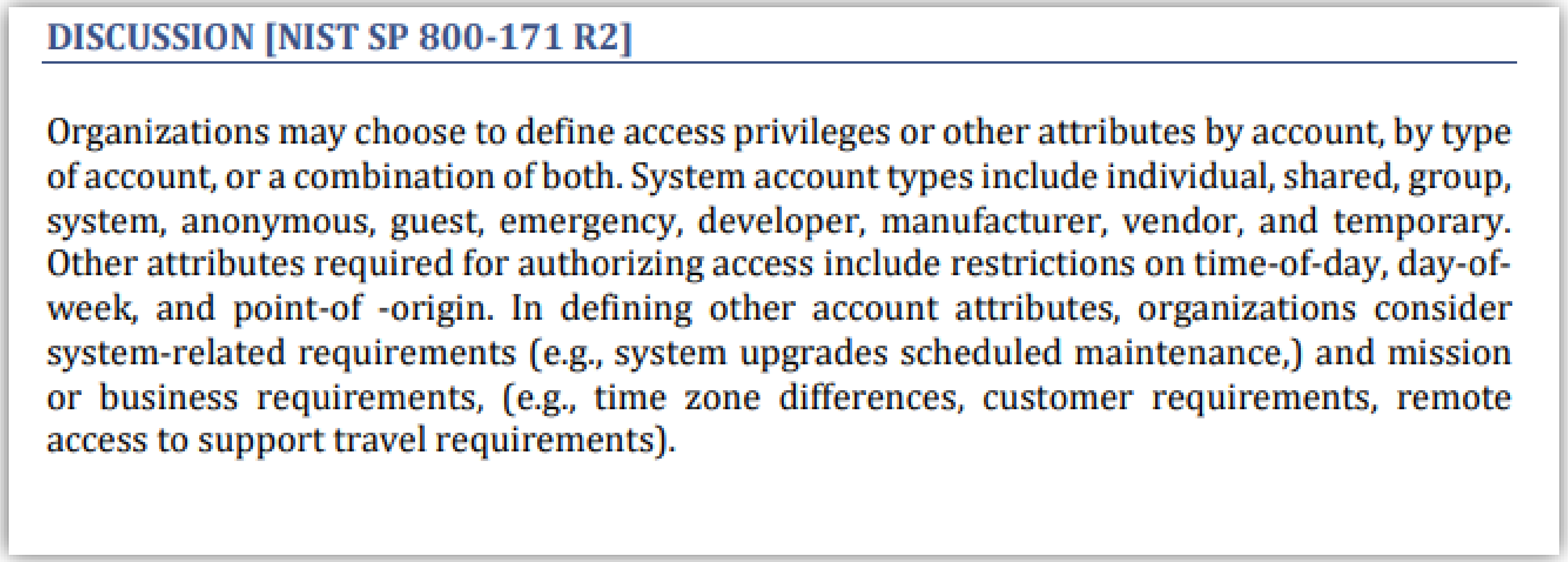
[SELECT FROM: Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing access control policy].

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

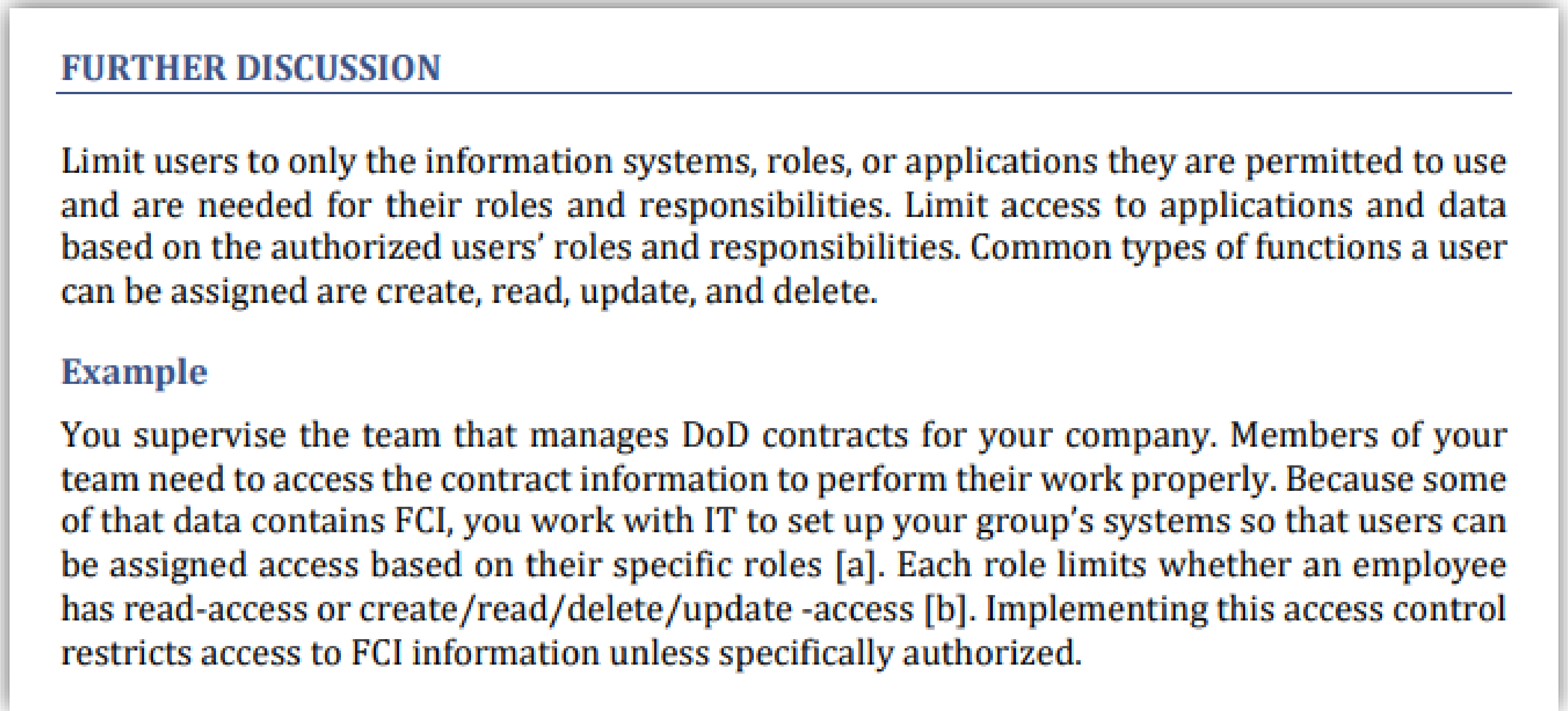


DISCUSSION [NIST SP 800-171 R2]

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of -origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.



FURTHER DISCUSSION

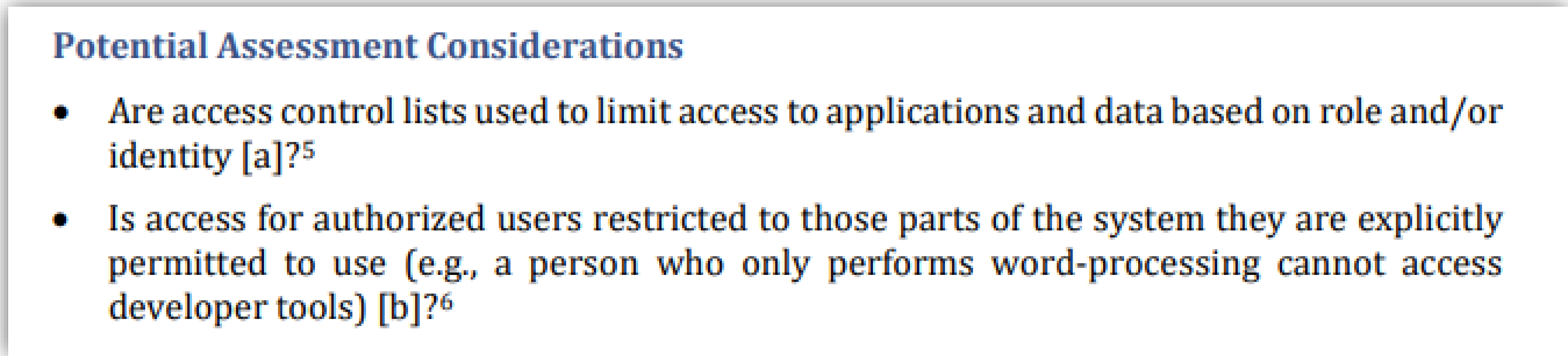
Limit users to only the information systems, roles, or applications they are permitted to use and are needed for their roles and responsibilities. Limit access to applications and data based on the authorized users' roles and responsibilities. Common types of functions a user can be assigned are create, read, update, and delete.

Example

You supervise the team that manages DoD contracts for your company. Members of your team need to access the contract information to perform their work properly. Because some of that data contains FCI, you work with IT to set up your group's systems so that users can be assigned access based on their specific roles [a]. Each role limits whether an employee has read-access or create/read/delete/update -access [b]. Implementing this access control restricts access to FCI information unless specifically authorized.

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

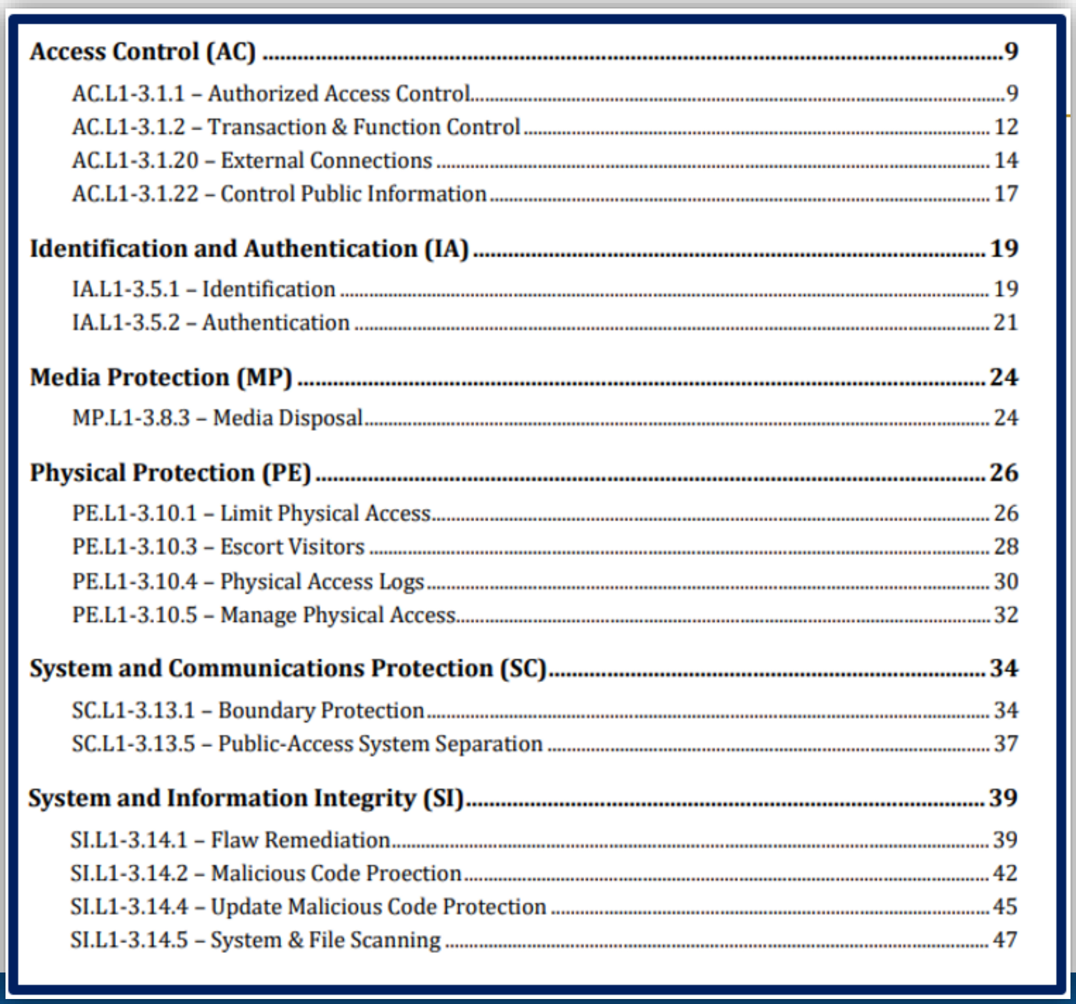


Potential Assessment Considerations

- Are access control lists used to limit access to applications and data based on role and/or identity [a]?[5]
- Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools) [b]?[6]

Now Repeat for each of the 17 Security Requirements

- Document your results
- Document your Evidence
- Set a schedule to update
- Ask your questions



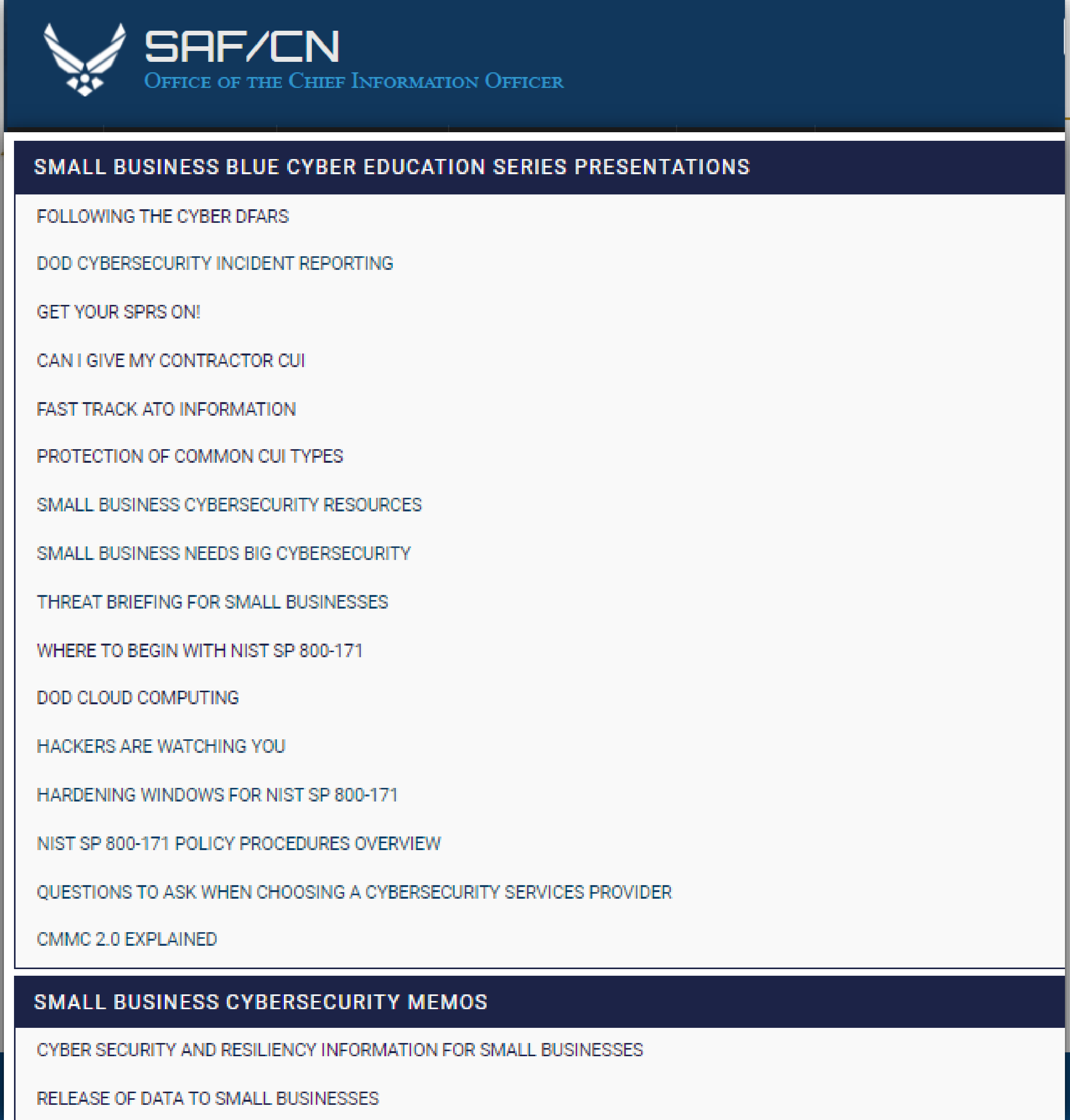
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and twenty other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - **Daily Office Hours** for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!
  - **Every Tuesday 1pm EST**, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg

The Blue Cyber Education Series for DAF Small Businesses on the DAF CISO webpage www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!

Every Tuesday 1pm EST, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg



SAF/CN
OFFICE OF THE CHIEF INFORMATION OFFICER

SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS

FOLLOWING THE CYBER DFARS

DOD CYBERSECURITY INCIDENT REPORTING

GET YOUR SPRS ON!

CAN I GIVE MY CONTRACTOR CUI

FAST TRACK ATO INFORMATION

PROTECTION OF COMMON CUI TYPES

SMALL BUSINESS CYBERSECURITY RESOURCES

SMALL BUSINESS NEEDS BIG CYBERSECURITY

THREAT BRIEFING FOR SMALL BUSINESSES

WHERE TO BEGIN WITH NIST SP 800-171

DOD CLOUD COMPUTING

HACKERS ARE WATCHING YOU

HARDENING WINDOWS FOR NIST SP 800-171

NIST SP 800-171 POLICY PROCEDURES OVERVIEW

QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES PROVIDER

CMMC 2.0 EXPLAINED

SMALL BUSINESS CYBERSECURITY MEMOS

CYBER SECURITY AND RESILIENCY INFORMATION FOR SMALL BUSINESSES

RELEASE OF DATA TO SMALL BUSINESSES