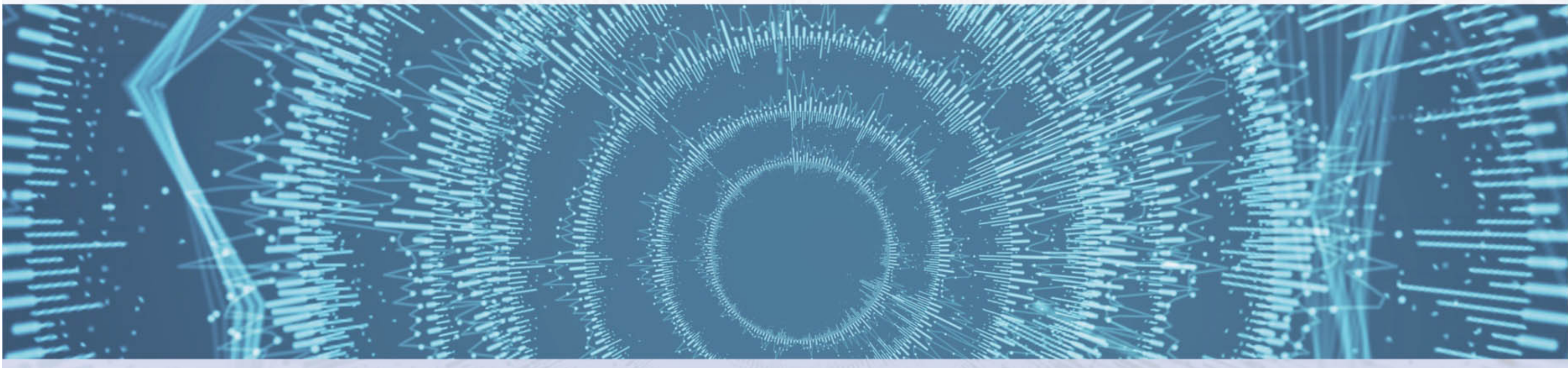
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



DRAFT

Version 0.6

November 7, 2019

NOTICES

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory, LLC, a University Affiliated Research Center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY AND JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY LLC MAKE NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL NOR ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM19-0824

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The United States Department of Defense (DoD) Office of the Under Secretary of Defense for Acquisition and Sustainment [OUSD(A&S)] is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of sensitive data – namely, Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), within the supply chain. The theft of hundreds of billions of dollars of intellectual property (IP) due to malicious cyber activity threatens the U.S. economy and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 [46]. Moreover, the Center for Strategic and International Studies estimates that the cost of cybercrime worldwide is approximately $600 billion [80]. The majority of this IP theft is directly attributable to poor cybersecurity maturity and ineffective implementation of controls necessary to protect sensitive data.

The sharing of FCI and CUI with DIB sector contractors expands the Department's attack surface because sensitive data is distributed beyond the DoD's information security boundary. Cybersecurity must become a foundation of DoD acquisition. Towards that end, OUSD(A&S) is working with DoD stakeholders, University-Affiliated Research Centers, Federally Funded Research and Development Centers, and industry to develop the Cybersecurity Maturity Model Certification (CMMC).

CMMC is a DoD certification process that measures a DIB sector company's ability to protect FCI and CUI. CMMC combines various cybersecurity standards and maps these best practices and processes to maturity levels, ranging from basic cyber hygiene to highly advanced practices. The CMMC effort builds upon existing regulation, specifically, 48 Code of Federal Regulations (CFR) 52.204-21 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, and incorporates practices from multiple sources such as NIST SP 800-171 rev 1, Draft NIST SP 800-171B, the United Kingdom's Cyber Essentials, and Australia's Essential Eight [4,11,12,47]. CMMC also adds a certification element to verify implementation of cybersecurity requirements. CMMC is designed to provide the DoD assurance that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for flow down to subcontractors in a multi-tier supply chain.

CMMC Version 0.4 was released for public review and comment in early September 2019. Based on this feedback, this version significantly reduces the model size, modifies the practices and processes, and provides clarifications and examples for CMMC Level 1.

DoD is releasing this latest version so that the public can review the draft model and begin to prepare for the eventual CMMC roll out. This document includes CMMC Levels 1-3 of the latest version of the CMMC Model (Appendix A) with clarifications for CMMC Level 1 in Appendix B. The updates to CMMC Levels 4-5 will be provided in the next public release.* These higher CMMC levels focus on reducing the risk of advanced persistent threats (APTs) and are intended to protect CUI associated with DoD critical programs and technologies. Section 2 describes the model framework, including levels, capability domains, and processes. Section 3 provides instructions on how to read the model. This document also provides key references, a glossary of terms, and a list of acronyms.

* CMMC Levels 4-5 are not included in this release because public comments are still being addressed.

2. CMMC MODEL FRAMEWORK

The CMMC model framework (Figure 1) categorizes cybersecurity best practices at the highest level by *domains*. Each domain is further segmented by a set of *capabilities*. Capabilities are achievements to ensure cybersecurity objectives are met within each domain. Companies will further demonstrate compliance with the required capabilities by demonstrating adherence to practices and processes, which have been mapped across the five maturity levels of CMMC. Under this context, *practices* will measure the technical activities required to achieve compliance with a given capability requirement, and *processes* will measure the maturity of a company's processes. Within each domain, DIB companies will be accredited under the CMMC only if they can demonstrate compliance with the required practices and demonstrate mature processes as required for the given CMMC level.

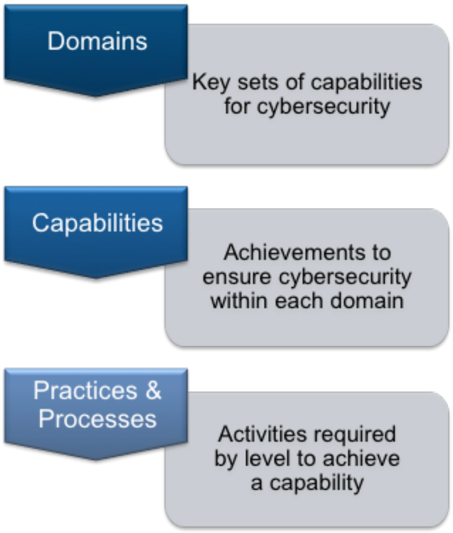

Domains
Key sets of capabilities for cybersecurity
Capabilities
Achievements to ensure cybersecurity within each domain
Practices & Processes
Activities required by level to achieve a capability

Figure 1. CMMC Model Framework

The next three subsections provide additional detail on the definitions of the CMMC levels, the domains and their capabilities, and process maturity expectations by CMMC level.

2.1 CMMC LEVELS

The CMMC model has five defined levels, each with a set of supporting practices and processes, illustrated in Figure 2. Practices range from Level 1 (basic cyber hygiene) and to proactive and advanced Levels 4 and 5. In parallel, processes range from being performed at Level 1, to being documented at Level 2, to being optimized across the organization at Level 5. To meet a specific CMMC level, an organization must meet the practices and processes within that level and below.

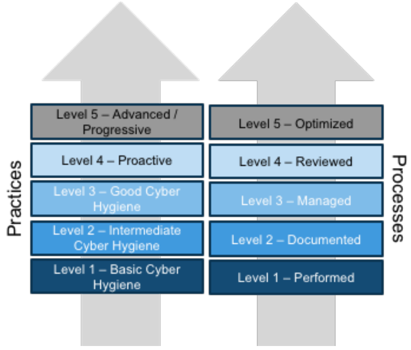


Figure 2. CMMC Level Descriptions

Each of the levels is described in more detail below, with descriptions summarized in Table 1.

2.1.1 Level 1

CMMC Level 1 focuses on basic cyber hygiene and consists of the safeguarding requirements specified in 48 CFR 52.204-21. The Level 1 practices establish a foundation for the higher levels of the model and must be completed by all certified organizations.

Not every domain within CMMC has Level 1 practices. At both this level and Level 2, organizations may be provided with FCI. FCI is information not intended for public release. It is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public.

While practices are expected to be performed, process maturity is not addressed at CMMC Level 1, and therefore, a CMMC Level 1 organization may have limited or inconsistent cybersecurity maturity.

2.1.2 Level 2

CMMC Level 2 focuses on intermediate cyber hygiene, creating a maturity-based progression for organizations to step from Level 1 to 3. This more advanced set of practices gives the organization greater ability to both protect and sustain their assets against more cyber threats compared to Level 1.

CMMC Level 2 also introduces the process maturity dimension of the model. At CMMC Level 2, an organization is expected to establish and document standard operating procedures, policies, and strategic plans to guide the implementation of their cybersecurity program.

2.1.3 Level 3

An organization assessed at CMMC Level 3 will have demonstrated good cyber hygiene and effective implementation of controls that meet the security requirements of NIST SP 800-171 Rev 1. Organizations that require access to CUI and/or generate CUI should achieve CMMC Level 3. CMMC Level 3 indicates a basic ability to protect and sustain an organization's assets and CUI; however, at CMMC Level 3, organizations will have challenges defending against advanced persistent threats (APTs).

For process maturity, a CMMC Level 3 organization is expected to adequately resource and review activities adherence to policy and procedures, demonstrating management of practice implementation.

2.1.4 Level 4 and Level 5

At CMMC Level 4 and 5, an organization has a substantial and proactive cybersecurity program. The organization has the capability to adapt their protection and sustainment activities to address the changing tactics, techniques, and procedures (TTPs) in use by APTs. For process maturity, the organization is expected to review and document activities for effectiveness and inform high-level management of any issues as well as ensure that process implementation has been generally optimized across the organization. The updates to CMMC Levels 4-5 will be provided in the next public release.

2.1.5 Summary of CMMC Levels

Table 1. Summary of CMMC Levels

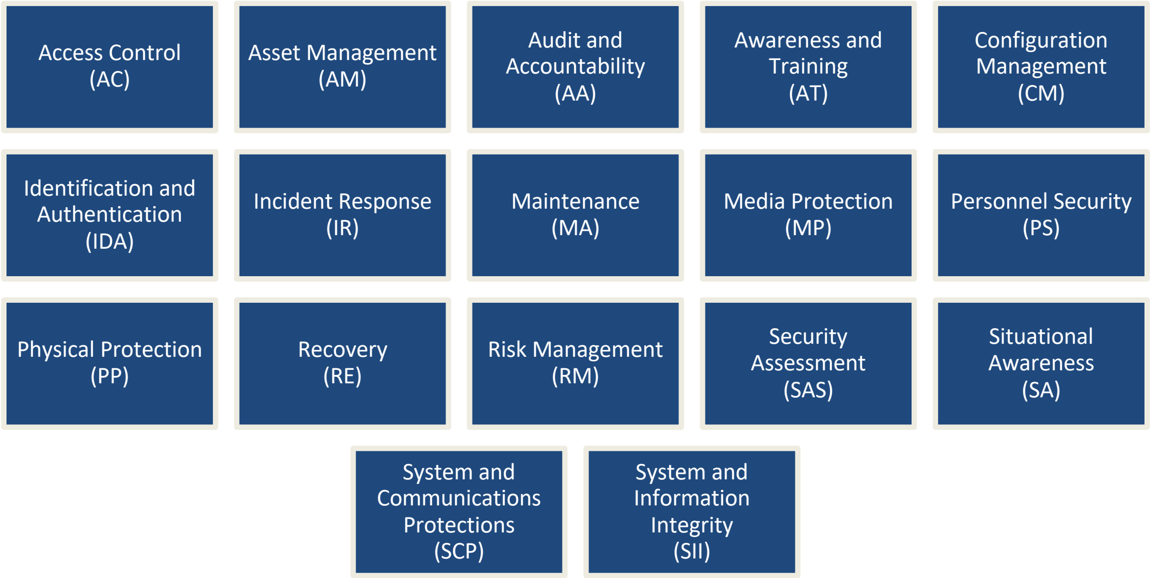
	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Technical Practices	Demonstrate basic cyber hygiene, as achieved by the Federal Acquisition Regulation (FAR)	Demonstrate intermediate cyber hygiene	Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements	Demonstrate a substantial and proactive cybersecurity program	Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats
Process Maturity	No process maturity	Standard operating procedures, policies, and plans are established for all practices	Activities are reviewed for adherence to policy and procedures and adequately resourced	Activities are reviewed effectiveness and management is informed of any issues	Activities are standardized across all applicable organizational units and identified improvements are shared

Note that adherence to CMMC processes and practices is cumulative. Once a practice is introduced in a level, it is a required practice for all levels above as well. For an organization to achieve Level 3, all the practices and processes defined in Levels 1, 2, and 3 must be achieved. Similarly, to achieve a specific level of CMMC, an organization must meet both the practices and processes within that level and below across all of the domains of the model. For example, an organization that scores a Level 3 on practice implementation and a Level 2 on process institutionalization will be assigned a CMMC Level of 2. Demonstration of practices and process institutionalization are equally important in CMMC and, thus, organizations must satisfy the defined requirements for both.

2.2 CMMC DOMAINS

The CMMC model consists of 17 domains. The majority of these CMMC domains originated from the FIPS 200 security-related areas and the NIST SP 800-171 control families. The CMMC model also includes the Asset Management, Recovery, and Situational Awareness domains.

These domains are shown in Figure 3 with their abbreviations as used in the model practice numbering system.



Access Control (AC)

Asset Management (AM)

Audit and Accountability (AA)

Awareness and Training (AT)

Configuration Management (CM)

Identification and Authentication (IDA)

Incident Response (IR)

Maintenance (MA)

Media Protection (MP)

Personnel Security (PS)

Physical Protection (PP)

Recovery (RE)

Risk Management (RM)

Security Assessment (SAS)

Situational Awareness (SA)

System and Communications Protections (SCP)

System and Information Integrity (SII)

Figure 3. CMMC Model Domains

Table 2 lists the capabilities for each domain. Each capability includes at least one practice at a specified level in the model. Appendix A contains Levels 1-3 of the model, including these practices. More detailed domain definitions are provided in the Appendix C Glossary.

Table 2. List of Capabilities for Each Domain

Domain	Capability
Access Control	Establish system access requirements
	Control internal system access
	Control remote system access
	Limit data access to authorized users and processes
Asset Management	Identify and document assets
Audit and Accountability	Define audit requirements
	Perform auditing
	Identify and protect audit information
	Review and manage audit logs
Awareness and Training	Conduct security awareness activities
	Conduct training
Configuration Management	Establish configuration baselines
	Perform configuration and change management
Identification and Authentication	Grant access to authenticated entities
Incident Response	Plan incident response
	Detect and report events
	Develop and implement a response to a declared incident
	Perform post incident reviews
	Test incident response
Maintenance	Manage maintenance
Media Protection	Identify and mark media
	Protect and control media
	Sanitize media
	Protect media during transport
Personnel Security	Screen personnel
	Protect federal contract information during personnel actions
Physical Protection	Limit physical access
Recovery	Manage back-ups
Risk Management	Identify and evaluate risk
	Manage risk
Security Assessment	Develop and manage a system security plan
	Define and manage controls
	Perform code reviews
Situational Awareness	Implement threat monitoring
Systems and Communications Protection	Define security requirements for systems and communications
	Control communications at system boundaries
System and Information Integrity	Identify and manage information system flaws
	Identify malicious content
	Perform network and system monitoring
	Implement advanced email protections

2.3 CMMC PROCESS MATURITY

Process maturity is the extent of institutionalization of practices at an organization. Table 3 lists the maturity processes expected to be performed by organizations at each of the five CMMC Levels. For example, a CMMC Level 3 organization must meet both the Level 3 defined practices, as well as the defined processes of Maturity Level (ML) 3. CMMC Version 1.0 will include tailored maturity processes for each domain. Additional guidance and clarification around assessment will also be provided in future iterations. Note that the nine processes are applied to each domain individually.

Table 3. Processes for each CMMC Maturity Level (ML)

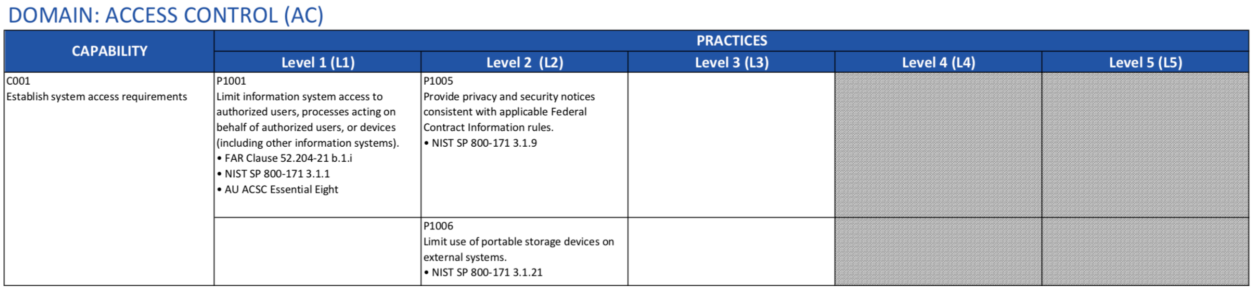
Process Maturity Level	Processes
ML 1: Performed	*There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.*
ML 2: Documented	1. Establish a policy that includes [DOMAIN NAME] 2. Establish practices to implement the [DOMAIN NAME] policy 3. Establish a plan that includes [DOMAIN NAME]
ML 3: Managed	1. Review [DOMAIN NAME] activities for adherence to policy and practices 2. Provide adequate resources for [DOMAIN NAME] activities
ML 4: Reviewed	1. Review and measure [DOMAIN NAME] activities for effectiveness 2. Inform high-level management of any issues with [DOMAIN NAME] activities
ML 5: Optimized	1. Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units 2. Share identified improvements to [DOMAIN NAME] activities across the organization

3. READING THE MODEL

The draft CMMC Model Version 0.6 represents the current iteration in the development of the model; note that this format may change ahead of the final version.

Figure 4 provides an excerpt of the Version 0.6 draft model. For each domain, the first column defines the set of expected capabilities. Each capability is assigned a unique number C###. The next five columns break out the five defined levels for CMMC and the associated practices. Each practice is assigned a unique number P1###.

Not every capability has practices at every level. However, once a practice is introduced, it applies to the level it is in and all higher levels. In the example below, there are no required practices at Levels 3 for this capability. As a result, the Level 3 cells are blank, but the practices in Level 1 and 2 are still required to achieve Level 3. Some levels may have more than one practice per capability. Using the same example, Level 2 contains two practices that must be satisfied, in addition to the Level 1 practice, to achieve Level 2 for this capability. CMMC Levels 4-5 are shown with hash marks and will be provided in the next public release.



DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight	P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules. • NIST SP 800-171 3.1.9		▨	▨
		P1006 Limit use of portable storage devices on external systems. • NIST SP 800-171 3.1.21		▨	▨

Figure 4. Example Model Capability with Practices from the AC Domain

Below each practice is a bulleted list of references that informed the development of the practice. These sources are not additional requirements for the model. Some practices have multiple references. Some practices, particularly those referenced to 'CMMC', were developed by the CMMC working team or through collaboration with industry.

Table 1 provides counts of the number of practices derived from key references. Some security requirements have not been included based on feedback regarding implementation challenges and costs.

Table 4. CMMC Model Version 0.6 Practices per Reference

CMMC Level	Total	48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B
Level 1	17	15	17	-
Level 2	58	-	51	-
Level 3	56	-	42	-
Level 4	62	-	-	17
Level 5	26	-	-	9
N/A - Excluded	-	-	-	7
Total	**219**	**15**	**110**	**33**

CMMC Model Version 1.0, to be released in late January 2020, will be in document form with clarifications for Levels 1-2. The draft Appendix B provides an example of the discussion and clarification material being developed. This material provides additional insights and examples. CMMC Model Version 1.0 will also include a mapping to the key references that informed model development, as shown above.

4. REFERENCES

1. 48 Code of Federal Regulations (CFR) 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, Federal Acquisition Regulation (FAR), 1 Oct 2016

2. CERT® Resilience Management Model (CERT RMM) Version 1.2, *A Maturity Model for Managing Operational Resilience*, Carnegie Mellon University Software Engineering Institute, February 2016

3. DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, October 2016

4. *Essential Eight Maturity Model*, Australian Cyber Security Centre (ACSC), July 2018

5. FIPS PUB 197, *Advanced Encryption Standard (AES)*, November 2001

6. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

7. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, Department of Commerce, March 2006

8. FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013

9. National Aerospace Standard (NAS) NAS9933, *Critical Security Controls for Effective Capability in Cyber Defense*, Aerospace Industries Association (AIA), 2018

10. NIST Cybersecurity Framework (CSF), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018

11. NIST Special Publication (SP) 800-171 Revision (Rev) 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, U.S. Department of Commerce National Institute of Standards and Technology (NIST), December 2016 (updated June 2018)

12. NIST SP 800-171B, *DRAFT Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets*, U.S. Department of Commerce National Institute of Standards and Technology (NIST), December 2016 (updated June 2018)

13. NIST SP 800-114 Rev. 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, July 2016

14. NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008

15. NIST SP 800-12 Rev. 1, *An Introduction to Information Security*, June 2017

16. NIST SP 800-123, *Guide to General Server Security*, July 2008

17. NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011 (Updated October 2019)

18. NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, October 2016

19. NIST SP 800-16, *Information Technology Security Training Requirements: a Role- and Performance-Based Model*, April 1998

20. NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016 (Updated March 2018)

21. NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015

22. NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016

23. NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006

24. NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012

25. NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001

26. NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (updated November 2010)

27. NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018

28. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011

29. NIST SP 800-41 Rev 1, *Guidelines on Firewalls and Firewall Policy*, September 2009

30. NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 2015)

31. NIST SP 800-57 Part 1 Rev. 4, *Recommendation for Key Management*, January 2016

32. NIST SP 800-57 Part 2 Rev. 1, *Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations*, May 2019

33. NIST SP 800-61, *Computer Security Incident Handling Guide*, August 2012

34. NIST SP 800-63-3, *Digital Identity Guidelines*, June 2017

35. NIST SP 800-66 Rev. 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008

36. NIST SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006

37. NIST SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015

38. NIST SP 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

39. NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013

40. NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006

41. NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2016

42. NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, December 2014

43. NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006

44. NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007

45. NIST SP 800-95, *Guide to Secure Web Services*, August 2007

46. U.S. Executive Office of the President, Council of Economic Advisers (CEA). *The Cost of Malicious Cyber Activity to the U.S. Economy*, available online at https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, February 2018

47. United Kingdom (UK) Cyber Essentials, National Cyber Security Centre (NCSC), available online https://www.cyberessentials.ncsc.gov.uk.

48. Center for Internet Security (CIS) Critical Security Controls version 7.1, available online at https://www.cisecurity.org/controls/, July 2019

49. ISO/IEC 27001:2013, *International Organization for Standardization (ISO): Information Security Management,* available online at: https://www.iso.org/isoiec-27001-information-security.html, 2019

50. National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 7298 Rev. 3, *Glossary of Key Information Security Terms*, July 2019

51. NISTIR 7298 Rev. 3, *Glossary of Key Information Security Terms*, July 2019

52. NISTIR 7316, *Assessment of Access Control Systems*, September 2006

53. NISTIR 7621 Rev. 1, *Small Business Information Security: The Fundamentals*, November 2016

54. NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012

55. NISTIR 7693, *Specification for Asset Identification 1.1*, June 2011

56. NISTIR 7694, *Specification for Asset Reporting Format 1.1*, June 2011

57. NISTIR 8011 Vol. 3, *Automation Support for Security Control Assessments: Software Asset Management*, December 2018

58. NISTIR 8053, *De-Identification of Personal Information*, October 2015

59. NISTIR 8074 Vol. 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, December 2015

60. NISTIR 8149, *Develop Trust Frameworks to Support Identity Federations*, January 2018

61. Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems from Insider Threat*, September 2016

62. CNSSD 505, *Supply Chain Risk Management (SCRM)*, August 2017

63. Committee on National Security Systems Instruction (CNSSI) 4009, *Committee on National Security Systems Glossary*, April 2015

64. CNSSI 1011, *Implementing Host-Based Security Capabilities on National Security Systems*, July 2013

65. CNSSI 4005, *Safeguarding COMSEC Facilities and Materials*, August 2011

66. Oxford Dictionary, *Oxford Dictionary of English 3rd Edition,* 2015

67. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, February 2013

68. Office of Management and Budget (OMB) M-17-09, *Management of Federal High Value Assets*, December 2016

69. New York State Society of CPAs (NYSSCPA), *Accounting Terminology Guide*, 2019

70. National Security Presidential Directive (NSPD) 54, *Cybersecurity Policy*, January 2008

71. Homeland Security Presidential Directive (HSPD) 23, *Cybersecurity Policy*, January 2008

72. NSA Central Security Service (NSA/CSS) Policy Manual 3-16, *Control of Communications Security (COMSEC)*, August 2005

73. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4949 Version 2, *Internet Security Glossary*, August 2007

74. DHS Cybersecurity and Infrastructure Security Agency (CISA) Sector Specific Plan (SSP), *Defense Industrial Base (DIB) Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* May 2007

75. DHS Baseline Risk Assessment, *Information Technology Sector Baseline Risk Assessment*, August 2009

76. Executive Order (E.O.) 13556, *Controlled Unclassified Information*, November 2010

77. DoD Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 2018

78. DoDI 5000.02, *Operation of the Defense Acquisition System*, January 2015

79. 44 U.S. Code Section 3542, *Public Printing and Documents: Definitions*, January 2012

80. Center for Strategic and International Studies (CSIS) and McAfee, *Economic Impact of Cybercrime - No Slowing Down*, February 2018

81. European Union General Data Protection Regulation (GDPR), online at https://eugdpr.org/

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight	P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules. • NIST SP 800-171 3.1.9			
		P1006 Limit use of portable storage devices on external systems. • NIST SP 800-171 3.1.21			
C002 Control internal system access	P1002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 3.1.2	P1007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 3.1.5 • UK NCSC Cyber Essentials	P1017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4		
		P1008 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 3.1.6 • UK NCSC Cyber Essentials	P1018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 3.1.7		
		P1009 Limit unsuccessful logon attempts. • NIST SP 800-171 3.1.8	P1019 Terminate (automatically) user sessions after a defined condition. • NIST SP 800-171 3.1.11		
		P1010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 3.1.10	P1020 Control connection of mobile devices. • NIST SP 800-171 3.1.18 • UK NCSC Cyber Essentials		
		P1011 Authorize wireless access prior to allowing such connections. • NIST SP 800-171 3.1.16			
		P1012 Protect wireless access using authentication and encryption. • NIST SP 800-171 3.1.17			
C003 Control remote system access		P1013 Monitor and control remote access sessions. • NIST SP 800-171 3.1.12	P1021 Authorize remote execution of privileged commands and remote access to security-relevant information. • NIST SP 800-171 3.1.15		

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
		P1014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. • NIST SP 800-171 3.1.13			
		P1015 Route remote access via managed access control points. • NIST SP 800-171 3.1.14			
C004 Limit data access to authorized users and processes	P1003 Verify and control/limit connections to and use of external information systems. • FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 3.1.20	P1016 Control the flow of Federal Contract Information in accordance with approved authorizations. • NIST SP 800-171 3.1.3 • UK NCSC Cyber Essentials	P1022 Encrypt CUI on mobile devices and mobile computing platforms. • NIST SP 800-171 3.1.19		
	P1004 Control information posted or processed on publicly accessible information systems. • FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 3.1.22				

DOMAIN: ASSET MANAGEMENT (AM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C005 Identify and document assets			P1035 Identify, categorize, and label all CUI data. • ISO/IEC 27001 A.8.2.1 • ISO/IEC 27001 A.8.2.2		
			P1036 Define procedures for the handling of CUI data. • ISO/IEC 27001 A.8.2.3		

DOMAIN: AUDIT AND ACCOUNTABILITY (AA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C007 Define audit requirements		P1041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. • NIST SP 800-171 3.3.2 • CERT RMM v1.2 MON:SG1.SP3	P1045 Review and update logged events. • NIST SP 800-171 3.3.3		
			P1046 Alert in the event of an audit logging process failure. • NIST SP 800-171 3.3.4		
C008 Perform auditing		P1042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. • NIST SP 800-171 3.3.1 • CERT RMM v1.2 MON:SG2.SP3	P1048 Collect audit logs into a central repository. • CMMC		
		P1043 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. • NIST SP 800-171 3.3.7			
C009 Identify and protect audit information			P1049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. • NIST SP 800-171 3.3.8 • CERT RMM v1.2 MON:SG2.SP3		
			P1050 Limit management of audit logging functionality to a subset of privileged users. • NIST SP 800-171 3.3.9 • CERT RMM v1.2 MON:SG2.SP2		
C010 Review and manage audit logs		P1044 Review audit logs. • CMMC	P1051 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. • NIST SP 800-171 3.3.5		
			P1052 Provide audit record reduction and report generation to support on-demand analysis and reporting. • NIST SP 800-171 3.3.6		

DOMAIN: AWARENESS AND TRAINING (AT)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C011 Conduct security awareness activities		P1056 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. • NIST SP 800-171 3.2.1 • CERT RMM v1.2 OTA:SG1.SP1	P1058 Provide security awareness training on recognizing and reporting potential indicators of insider threat. • NIST SP 800-171 3.2.3		
C012 Conduct training		P1057 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. • NIST SP 800-171 3.2.2 • CERT RMM v1.2 OTA:SG4.SP1			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C013 Establish configuration baselines		P1061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. • NIST SP 800-171 3.4.1 • CERT RMM v1.2 KIM:SG5.SP2 • UK NCSC Cyber Essentials			
		P1062 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. • NIST SP 800-171 3.4.6 • UK NCSC Cyber Essentials			
		P1063 Control and monitor user-installed software. • NIST SP 800-171 3.4.9			
C014 Perform configuration and change management		P1064 Establish and enforce security configuration settings for information technology products employed in organizational systems. • NIST SP 800-171 3.4.2 • UK NCSC Cyber Essentials	P1067 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. • NIST SP 800-171 3.4.5 • UK NCSC Cyber Essentials		
		P1065 Track, review, approve, or disapprove, and log changes to organizational systems. • NIST SP 800-171 3.4.3 • CERT RMM v1.2 KIM:SG5.SP2 • AU ACSC Essential Eight	P1068 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. • NIST SP 800-171 3.4.7 • UK NCSC Cyber Essentials		
		P1066 Analyze the security impact of changes prior to implementation. • NIST SP 800-171 3.4.4	P1069 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. • NIST SP 800-171 3.4.8 • UK NCSC Cyber Essentials		

DOMAIN: IDENTIFICATION AND AUTHENTICATION (IDA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C015 Grant access to authenticated entities	P1076 Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 3.5.1	P1078 Enforce a minimum password complexity and change of characters when new passwords are created. • NIST SP 800-171 3.5.7 • UK NCSC Cyber Essentials	P1083 Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. • NIST SP 800-171 3.5.3 • AU ACSC Essential Eight		
	P1077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 3.5.2 • UK NCSC Cyber Essentials	P1079 Prohibit password reuse for a specified number of generations. • NIST SP 800-171 3.5.8	P1084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 3.5.4		
		P1080 Allow temporary password use for system logons with an immediate change to a permanent password. • NIST SP 800-171 3.5.9	P1085 Prevent the reuse of identifiers for a defined period. • NIST SP 800-171 3.5.5		
		P1081 Store and transmit only cryptographically-protected passwords. • NIST SP 800-171 3.5.10	P1086 Disable identifiers after a defined period of inactivity. • NIST SP 800-171 3.5.6		
		P1082 Obscure feedback of authentication information. • NIST SP 800-171 3.5.11			

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C016 Plan incident response		P1092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. • NIST SP 800-171 3.6.1			
C017 Detect and report events		P1093 Detect and report events. • CERT RMM v1.2 IMC:SG2.SP1			
		P1094 Analyze and triage events to support event resolution and incident declaration. • CERT RMM v1.2 IMC:SG2.SP4			
C018 Develop and implement a response to a declared incident		P1096 Develop and implement responses to declared incidents according to pre-defined procedures. • CERT RMM v1.2 IMC:SG4.SP2	P1098 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. • NIST SP 800-171 3.6.2		
C019 Perform post incident reviews		P1097 Perform root cause analysis on incidents to determine underlying causes. • CERT RMM v1.2 IMC:SG5.SP1			
C020 Test incident response			P1099 Test the organizational incident response capability. • NIST SP 800-171 3.6.3		

DOMAIN: MAINTENANCE (MA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C021 Manage maintenance		P1111 Perform maintenance on organizational systems. • NIST SP 800-171 3.7.1 • CERT RMM v1.2 TM:SG5.SP2	P1115 Ensure equipment removed for off-site maintenance is sanitized of any CUI. • NIST SP 800-171 3.7.3		
		P1112 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. • NIST SP 800-171 3.7.2	P1116 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. • NIST SP 800-171 3.7.4		
		P1113 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. • NIST SP 800-171 3.7.5			
		P1114 Supervise the maintenance activities of personnel without required access authorization. • NIST SP 800-171 3.7.6			

DOMAIN: MEDIA PROTECTION (MP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C022 Identify and mark media			P112 Mark media with necessary CUI markings and distribution limitations. • NIST SP 800-171 3.8.4 • CERT RMM v1.2 MON:SG2.SP4		
C023 Protect and control media		P1119 Protect (i.e., physically control and securely store) system media containing Federal Contract Information, both paper and digital. • NIST SP 800-171 3.8.1 • CERT RMM v1.2 KIM:SG2.SP2	P1123 Prohibit the use of portable storage devices when such devices have no identifiable owner. • NIST SP 800-171 3.8.8 • CERT RMM v1.2 MON:SG2.SP4		
		P1120 Limit access to Federal Contract Information on system media to authorized users. • NIST SP 800-171 3.8.2 • CERT RMM v1.2 MON:SG2.SP4			
		P1121 Control the use of removable media on system components. • NIST SP 800-171 3.8.7 • CERT RMM v1.2 MON:SG2.SP4			
C024 Sanitize media	P1118 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. • FAR Clause 52.204-21 b.1.vii • NIST SP 800-171 3.8.3				
C025 Protect media during transport			P1124 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. • NIST SP 800-171 3.8.5		
			P1125 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 3.8.6		

DOMAIN: PERSONNEL SECURITY (PS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C026 Screen personnel		P1127 Screen individuals prior to authorizing access to organizational systems containing Federal Contract Information. • NIST SP 800-171 3.9.1 • CERT RMM v1.2 HRM:SG2.SP1			
C027 Protect federal contract information during personnel actions		P1128 Ensure that organizational systems containing Federal Contract Information are protected during and after personnel actions such as terminations and transfers. • NIST SP 800-171 3.9.2 • CERT RMM v1.2 HRM:SG4.SP2			

DOMAIN: PHYSICAL PROTECTION (PP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C028 Limit physical access	P1131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. • FAR Clause 52.204-21 b.1.viii • NIST SP 800-171 3.10.1 • CERT RMM v1.2 KIM:SG4.SP2	P1135 Protect and monitor the physical facility and support infrastructure for organizational systems. • NIST SP 800-171 3.10.2 • CERT RMM v1.2 KIM:SG4.SP2	P1136 Enforce safeguarding measures for CUI at alternate work sites. • NIST SP 800-171 3.10.6	▨	▨
	P1132 Escort visitors and monitor visitor activity. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 3.10.3			▨	▨
	P1133 Maintain audit logs of physical access. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 3.10.4			▨	▨
	P1134 Control and manage physical access devices. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 3.10.5 • CERT RMM v1.2 KIM:SG4.SP2			▨	▨

DOMAIN: RECOVERY (RE)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C029 Manage back-ups		P1137 Regularly perform and test data back-ups. • AU ACSC Essential Eight • ISO/IEC 27001 A.12.3.1 • NIST CSF v1.1 PR.IP-4 • CIS Controls v7.1 10.1 and 10.3	P1139 Regularly perform complete and comprehensive data back-ups and store them off-site and offline. • CIS Controls v7.1 10.1, 10.2, and 10.5	▨	▨
		P1138 Protect the confidentiality of backup Federal Contract Information at storage locations. • NIST SP 800-171 3.8.9 • CERT RMM v1.2 MON:SG2.SP4		▨	▨

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C031 Identify and evaluate risk		P1141 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Federal Contract Information. • NIST SP 800-171 3.11.1 • CERT RMM v1.2 RISK:SG4	P1144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria. • CERT RMM v1.2 RISK:SG3 and SG4.SP3		
		P1142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. • NIST SP 800-171 3.11.2			
C032 Manage risk		P1143 Remediate vulnerabilities in accordance with risk assessments. • NIST SP 800-171 3.11.3 • CERT RMM v1.2 VAR:SG3.SP1	P1146 Develop and implement risk mitigation plans. • CERT RMM v1.2 RISK:SG5.SP1		
			P1147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. • CMMC		

DOMAIN: SECURITY ASSESSMENT (SAS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C034 Develop and manage a system security plan		P1157 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 3.12.4			
C035 Define and manage controls		P1158 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. • NIST SP 800-171 3.12.1	P1161 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. • NIST SP 800-171 3.12.3		
		P1159 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. • NIST SP 800-171 3.12.2			
C036 Perform code reviews			P1162 Employ code reviews of enterprise software developed for internal use to identify areas of concern that require additional improvements. • CMMC		

DOMAIN: SITUATIONAL AWARENESS (SA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C037 Implement threat monitoring			P1169 Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. • CMMC	▨	▨

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C039 Define security requirements for systems and communications		P1177 Employ FIPS-validated cryptography when used to protect the confidentiality of Federal Contract Information. • NIST SP 800-171 3.13.11	P1180 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. • NIST SP 800-171 3.13.2		
		P1178 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. • NIST SP 800-171 3.13.12	P1181 Separate user functionality from system management functionality. • NIST SP 800-171 3.13.3 • AU ACSC Essential Eight		
		P1179 Use encrypted sessions for the management of network devices. • CIS Controls v7.1 11.5	P1182 Prevent unauthorized and unintended information transfer via shared system resources. • NIST SP 800-171 3.13.4		
			P1183 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). • NIST SP 800-171 3.13.6		
			P1184 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). • NIST SP 800-171 3.13.7		
			P1185 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 3.13.8		
			P1186 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. • NIST SP 800-171 3.13.9		
			P1187 Establish and manage cryptographic keys for cryptography employed in organizational systems. • NIST SP 800-171 3.13.10		

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
			P1188 Control and monitor the use of mobile code. • NIST SP 800-171 3.13.13 • AU ACSC Essential Eight		
			P1189 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. • NIST SP 800-171 3.13.14		
			P1190 Protect the authenticity of communications sessions. • NIST SP 800-171 3.13.15		
			P1191 Protect the confidentiality of CUI at rest. • NIST SP 800-171 3.13.16		
C040 Control communications at system boundaries	P1175 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. • FAR Clause 52.204-21 b.1.x • NIST SP 800-171 3.13.1 • UK NCSC Cyber Essentials		P1192 Implement Domain Name System (DNS) filtering services. • CMMC • CIS Controls v7.1 7.7		
	P1176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. • FAR Clause 52.204-21 b.1.xi • NIST SP 800-171 3.13.5 • UK NCSC Cyber Essentials		P1193 Implement a policy restricting the publication of CUI on publically accessible websites (e.g., Forums, LinkedIn, Facebook, Twitter, etc.). • CMMC		

DOMAIN: SYSTEM AND INFORMATIONAL INTEGRITY (SII)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C041 Identify and manage information system flaws	P1210 Identify, report, and correct information and information system flaws in a timely manner. • FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 3.14.1 • UK NCSC Cyber Essentials • AU ACSC Essential Eight	P1214 Monitor system security alerts and advisories and take action in response. • NIST SP 800-171 3.14.3 • NIST CSF v1.1 RS.AN-5			
C042 Identify malicious content	P1211 Provide protection from malicious code at appropriate locations within organizational information systems. • FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 3.14.2 • AU ACSC Essential Eight				
	P1212 Update malicious code protection mechanisms when new releases are available. • FAR Clause 52.204-21 b.1.xiv • NIST SP 800-171 3.14.4				
	P1213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. • FAR Clause 52.204-21 b.1.xv • NIST SP 800-171 3.14.5				
C043 Perform network and system monitoring		P1216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. • NIST SP 800-171 3.14.6	P1218 Employ spam protection mechanisms at information system access entry and exit points. • CMMC		
		P1217 Identify unauthorized use of organizational systems. • NIST SP 800-171 3.14.7			
C044 Implement advanced email protections			P1219 Implement DNS or asymmetric cryptography email protections. • CMMC		
			P1220 Utilize email sandboxing to detect or block potentially malicious email attachments. • CIS Controls v7.1 7.10		

PROCESS MATURITY (ML)

MATURITY CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
MC01 Improve [DOMAIN NAME] activities		MP001 Establish a policy that includes [DOMAIN NAME].	MP004 Review [DOMAIN NAME] activities for adherence to policy and practices.	▨	▨
		MP002 Establish practices to implement the [DOMAIN NAME] policy.	MP005 Provide adequate resources for [DOMAIN NAME] activities.	▨	▨
		MP003 Establish a plan that includes [DOMAIN NAME].		▨	▨

APPENDIX B. CMMC LEVEL 1 DISCUSSION AND CLARIFICATION

Introduction

This draft provides discussion and clarifications for the CMMC Level 1 practices that map to the safeguarding requirements specified in 48 CFR 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems* and the associated security requirements in NIST SP 800-171 Rev 1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

Note that the clarification examples are intended only to help explain the practices and do not reflect guidance.

Access Control (AC) P1001: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

REFERENCES

- FAR Clause 52.204-21 b.1.i
- NIST SP 800-171 3.1.1
- AU ACSC Essential Eight
- CMMC AC-C001-P1001 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

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

CLARIFICATION

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

A coworker from the marketing department tells you their boss wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

Access Control (AC) P1002: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

REFERENCES

- FAR Clause 52.204-21 b.1.ii
- NIST SP 800-171 3.1.2
- CMMC AC-C002-P1002 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

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).

CLARIFICATION

Make sure to limit users/employees to only the systems, roles, or applications they are permitted to use and that are needed for their job.

Example

You are in charge of payroll for the company and need access to certain company financial information and systems. You work with IT to set up the system so that when users log onto the company's network, only those employees you allow can use the payroll applications and access payroll data. Because of this good access control, your coworkers in the Shipping Department cannot access information about payroll or paychecks.

Access Control (AC) P1003: Verify and control/limit connections to and use of external information systems.

REFERENCES

- FAR Clause 52.204-21 b.1.iii
- NIST SP 800-171 3.1.20
- CMMC AC-C004-P1003 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of Federally Contracted Information, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

DISCUSSION (continued) [DRAFT NIST SP 800-171R2]

Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of Federally Contracted Information across an organization, the organization may have systems that process Federally Contracted Information and others that do not. And among the systems that process Federally Contracted Information there are likely access restrictions for Federally Contracted Information that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

CLARIFICATION

Make sure to control and manage connections between your company network and outside networks, such as the public internet or a network that does not belong to your company. Be aware of applications that can be run by outside systems. Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information. You can also choose to limit how and when your network is connected to outside systems and/or decide that only certain employees can connect to outside systems from network resources.

Example

You help manage IT for your employer. You and your coworkers are working on a big proposal, and all of you will put in extra hours over the weekend to get it done. Part of the proposal includes Federal Contract Information, or FCI. FCI is information that you or your company get from doing work for the Federal government. Because FCI is not shared publicly, you remind your coworkers to use their company laptops, not personal laptops or tablets, when working on the proposal over the weekend.

Access Control (AC) P1004: Control information posted or processed on publicly accessible information systems.

REFERENCES

- FAR Clause 52.204-21 b.1.iv
- NIST SP 800-171 3.1.22
- CMMC AC-C004-P1004 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

CLARIFICATION

Do not allow sensitive information, including FCI, to become public. It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website. Limit and control information that is posted on your company's website(s) that can be accessed by the public.

Example

You are head of marketing for your company and want to become better known by your customers. So, you decide to start issuing press releases about your company projects. Your company gets Federal Contract Information, or FCI, from doing work for the Federal government. FCI is information that is not shared publicly. Because you recognize the need to control sensitive information, including FCI, you carefully review all information before posting it on the company website or releasing to the public. You allow only certain employees to post to the website.

Identification and Authentication (IDA) P1076: Identify information system users, processes acting on behalf of users, or devices.

REFERENCES

- FAR Clause 52.204-21 b.1.v
- NIST SP 800-171 3.5.1
- CMMC IDA-C015-P1076 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Common device identifiers include media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. [SP 800-63-3] provides guidance on digital identities.

CLARIFICATION

Authentication helps you to know who is using or viewing your system. Make sure to assign individual, unique identifiers, like user names, to all employees/users who access company systems. Confirm the identities of users, processes, or devices before allowing them access to the company's information system-usually done through passwords.

Example

You lead a project with the Department of Defense (DoD) for your small company and want to make sure that all employees working on the project can log on to the company system to see important information about the project. You also want to prevent employees who are not working on the DoD project from being able to access the information. You set up the system so that when an employee logs on, the system uniquely identifies each person, then determines the appropriate level of access.

Identification and Authentication (IDA) P1077: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

REFERENCES

- FAR Clause 52.204-21 b.1.vi
- NIST SP 800-171 3.5.2
- UK NCSC Cyber Essentials
- CMMC IDA-C015-P1077 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords. [SP 800-63-3] provides guidance on digital identities.

CLARIFICATION

Before you let a person or a device have access to your system, you need to verify that the user or device is who or what it claims to be. This verification is called authentication. The most common way to verify identity is using a username and a hard-to-guess password.

A more mature way of verification is multifactor authentication, which is checking more than one factor before a user can get on the system. Every time someone accesses the system, you check at least two factors. Example factors include:

- something the user knows or has memorized, like a PIN or a password
- something the user possesses, like a token or a smart card, or
- something the user “is,” like the fingerprint or a face scan used by modern smartphones.

CLARIFICATION *(continued)*

Some devices ship with default usernames and passwords. For example, some devices ship so that when you first logon to the device, the username is “admin” and the password is “admin”. When you have devices with this type of default username and password, you need to change the default password to a unique password you create. Default passwords are well known to the public, and easily found in a search. So, these default passwords would be easy for an unauthorized person to guess and use to gain access to your system.

Example

You are in charge of purchasing for your company. You know that some devices, such as laptops, come with a default username and a default password. Last week, your coworker in the Engineering Department received a laptop with the default username “admin” and default password “admin”. You remind the coworker to be sure to delete the default account details, or change the default password to a unique password. You also explain that default passwords are easily found in an internet search engine. So, it would be easy for an unauthorized person to guess and use the default password to gain access to the system.

Media Protection (MP) P1118: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

REFERENCES

- FAR Clause 52.204-21 b.1.vii
- NIST SP 800-171 3.8.3
- CMMC MP-C024-P1118 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization.

Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information. [SP 800-88] provides guidance on media sanitization.

CLARIFICATION

In this case, “media” can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones. It is important to see what information is on these types of media. If there is Federal contract information (FCI)—information you or your company got doing work for the Federal government that is not shared publicly)—you or someone in your company should do one of two things before throwing the media away:

- clean or purge the information, if you want to reuse the device, or
- shred or destroy the device so it cannot be read.

See NIST Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization* for more information.

CLARIFICATION ***(continued)***

Example

You are moving into a new office. As you pack for the move, you find some of your old CDs in a file cabinet. When you load the CDs into your computer drive, you see that one has information about an old project your company did for the Department of Defense (DoD). Rather than throw the CD in the trash, you make sure that it is shredded.

Physical Protection (PP) P1131: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

REFERENCES

- FAR Clause 52.204-21 b.1.viii
- NIST SP 800-171 3.10.1
- CERT RMM v1.2 KIM:SG4.SP2
- CMMC PP-C028-P1131 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

CLARIFICATION

Think about what parts of your physical space (office, plant, factory, etc.), what equipment, including the network, need to be protected from physical contact. For those parts of your company where you want only specific employees to have physical access to, monitor or limit who is able to enter those spaces with badges, key cards, etc.

Example

You work for a small company as the project manager for a Department of Defense (DoD) project. The project requires special equipment that should be used only by project team members. You work with your boss to put locks on the doors to your area. This restricts access to the room to only those employees who work on the DoD project.

Physical Protection (PP) P1132: Escort visitors and monitor visitor activity.

REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.3
- CMMC PP-C028-P1132 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

CLARIFICATION

Do not allow visitors, even those people you know well, to walk around your facility without an escort. Make sure that all non-employees wear special visitor badges and/or are escorted by an employee at all times while on your property.

Example

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office. You know this person well and trust them, but are not sure why they are in the building. You stop to talk, and the person explains that they are supposed to meet the coworker for lunch, but cannot remember where the lunchroom is. You offer to walk the person back to the reception area to get a visitor badge and wait until someone can escort them to the lunch room. You report this incident, and the company decides to install a badge reader at the main door so visitors cannot enter without an escort.

Physical Protection (PP) P1133: Maintain audit logs of physical access.

REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.4
- CMMC PP-C028-P1133 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

CLARIFICATION

Make sure you have a record of who is accessing both your facility (office, plant, factory, etc.) and your equipment. You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility.

Example

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company is growing, and sometimes it's hard to know who is coming and going from the lunch area. You work with your boss, the company founder, and ask all non-employees to sign in at the reception area, then sign out when they leave. Employees can have badges or key cards that enable tracking and logging access to the company facilities.

Physical Protection (PP) P1134: Control and manage physical access devices.

REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.5
- CERT RMM v1.2 KIM:SG4.SP2
- CMMC PP-C028-P1134 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Physical access devices include keys, locks, combinations, and card readers.

CLARIFICATION

Controlling physical access devices like locks, badging, key cards, etc. is just as important as monitoring and limiting who is able to physically access certain equipment. Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.

Example

A team member retired last week and forgot to turn in company items, including an identification badge and office keys. The project requires special equipment that should be used only by project team members. Before you begin looking for a replacement employee, you make sure to change the locks on the doors to the project area. You also disable the retired team member’s badge.

System and Communication Protection (SCP) P1175: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of information systems.

REFERENCES

- FAR Clause 52.204-21 b.1.x
- NIST SP 800-171 3.13.1
- UK NCSC Cyber Essentials
- CMMC SCP-C040-P1175 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. [SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

CLARIFICATION

Just as your office or plant has fences and locks for protection from the outside, and uses badges and keycards to keep non-employees out, your company’s IT network or system has boundaries that must be protected. Many companies use a web proxy and a firewall.

CLARIFICATION *(continued)*

Web Proxy

When an employee uses a company computer to go to a website, a web proxy makes the request on the user's behalf, looks at the web request, and decides if it should let the employee go to the website.

Firewall

A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company's network. A firewall stops unwanted traffic on the internet from passing through an outside "fence" to the company's networks and information systems.

If your company is large enough, you might want to monitor, control, or protect one part of the company enterprise/network from the other. This can also be done with a firewall. You may want to do this to stop adversaries, hackers, or disgruntled employees from entering your network and causing damage.

Example

You are setting up the new network for your company, and want to keep the company's information and resources safe. You make sure to buy a router—a hardware device that routes data from a local area network (LAN) to another network connection—with a built-in firewall, then configure it to limit access to trustworthy sites. Some of your coworkers complain that they cannot get onto to certain websites. You explain that the new network blocks websites that are known for spreading malware.

System and Communication Protection (SCP) P1176: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

REFERENCES

- FAR Clause 52.204-21 b.1.xi
- NIST SP 800-171 3.13.5
- UK NCSC Cyber Essentials
- CMMC SCP-C040-P1176 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

CLARIFICATION

Separate the publicly accessible systems from the internal systems that need to be protected. Do not place the internal systems on the same network as the publicly accessible systems.

A network or part of a network that is separated (sometimes physically) from an internal network is called a demilitarized zone (DMZ). A DMZ is a host or part of a network put in a “neutral zone” between an organization’s internal network (the protected side) and a larger network, like the internet. To separate a subnetwork physically, your company may put in boundary control devices (i.e., routers, gateways, firewalls). This can also be done on a cloud network that can be separated from the rest of the network.

A DMZ can add an extra layer of security to your company’s LAN, because an external network node can reach only what is permitted to be accessed in the DMZ.

CLARIFICATION *(continued)*

Example

The head of recruiting wants to launch a website to post job openings and allow the public to download an application form. After some discussion, your team realizes it needs to use a router and firewall to create a DMZ to do this. You host the server separately from the company’s internal network, and make sure the network has the correct security firewall rules. Your company gets a lot of great candidates for the open jobs, and the company’s internal network is protected.

System and Informational Integrity (SII) P1210: Identify, report, and correct information system flaws in a timely manner.

REFERENCES

- FAR Clause 52.204-21 b.1.xii
- NIST SP 800-171 3.14.1
- UK NCSC Cyber Essentials
- AU ACSC Essential Eight
- CMMC SII-C041-P1210 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

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. [SP 800-40] provides guidance on patch management technologies.

CLARIFICATION

Be aware of problems in the software and computer equipment your company uses. Consider purchasing support from your hardware and software vendors/suppliers, getting patches, and signing up for IT newsletters with updates about common problems or weaknesses in software. Install security updates promptly.

Example

You have many responsibilities at your company, including IT. You know that malware, ransomware, and viruses can be a big problem for small companies. You make sure to enable all security updates for your software, and purchase the maintenance packages for new hardware and operating systems.

System and Informational Integrity (SII) P1211: Provide protection from malicious code at appropriate locations within organizational information systems.

REFERENCES

- FAR Clause 52.204-21 b.1.xiii
- NIST SP 800-171 3.14.2
- AU ACSC Essential Eight
- CMMC SII-C042-P1211 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Designated locations include system entry and exit points which may include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. [SP 800-83] provides guidance on malware incident prevention.

CLARIFICATION

You can protect your company’s valuable IT system by stopping malicious code at designated locations in your system. Malicious code is program code that purposefully creates an unauthorized function or process that will have a negative impact on the confidentiality, integrity, or availability of an information system. A designated location may be your network device or your computer.

CLARIFICATION *(continued)*

Malicious code includes the following, which can be hidden in email, email attachments, web access:

- Viruses, programs designed to damage, steal information, change data, send email, show messages, or any combination of these things.
- Spyware, a program designed to gather information about a person's activity in secret, and is usually installed without the person knowing when they click on a link.
- A Trojan Horse, a type of malware made to look like legitimate/real software, and used by cyber criminals to get access to a company's systems

By using anti-malware tools, you can stop or lessen the impact of malicious code.

Example

You are buying a new computer for your small business and want to protect your company's information from viruses, spyware, etc. You buy and install anti-malware software.

System and Informational Integrity (SII) P1212: Update malicious code protection mechanisms when new releases are available.

REFERENCES

- FAR Clause 52.204-21 b.1.xiv
- NIST SP 800-171 3.14.4
- CMMC SII-C042-P1212 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other.

CLARIFICATION

You can protect your company's valuable IT systems by staying up to date on new security releases that stop malicious code and monitoring the system regularly. Malicious code is program code that is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.

Example

You bought a new computer for your small business. You know that you need to protect your company's information from viruses, spyware, etc. So, you also purchased and installed anti-malware software. You configure the software to automatically update to the latest antivirus code and definitions of all known malware.

System and Informational Integrity (SII) P1213: Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

REFERENCES

- FAR Clause 52.204-21 b.1.xv
- NIST SP 800-171 3.14.5
- CMMC SII-C042-P1213 L1

DISCUSSION [DRAFT NIST SP 800-171R2]

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. Many technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

CLARIFICATION

Companies should use anti-malware software to scan and identify viruses in their computer systems, and have a plan for how often scans are conducted. Real-time scans will look at the system whenever new files are downloaded, opened, and saved. Periodic scans check previously saved files against updated malware information.

CLARIFICATION *(continued)*

Example

While cleaning up your office, you find your old thumb drive. You are not sure if you should use it. Then you remember something: Your company just purchased anti-malware software that auto-updates with the latest antivirus code and definitions of all known malware. With this in mind, you decide to plug in the thumb drive. The new anti-malware software scans the thumb drive, finds a virus, then deletes the file.

APPENDIX C: GLOSSARY

This glossary of terms used in the CMMC model has been derived from multiple sources as cited.

Access
Ability to make use of any information system (IS) resource.

Source: CNSSI 4009, NIST SP 800-32, NIST SP 800-161, NISTIR 7298

Access Authority
An entity responsible for monitoring and granting access privileges for other authorized entities.

Source: CNSSI 4009

Access Control
The process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Source: FIPS 201, CNSSI 4009

Access Control Policy (Access Management Policy)
The set of rules that define the conditions under which an access may take place.

Source: NISTIR 7316

Access Profile
Association of a user with a list of protected objects the user may access.

Source: CNSSI 4009

Accountability
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Source: NIST SP 800-27

Administrative Safeguards
Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Source: NIST SP 800-66 Rev 1

Advanced Persistent Threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

- pursues its objectives repeatedly over an extended period of time;
- adapts to defenders' efforts to resist it; and
- is determined to maintain the level of interaction needed to execute its objectives.

Source: NIST SP 800-39

Adversary
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Source: CNSSI 4009

Adversarial Assessment
Assesses the ability of a unit equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary.

Source: DoDI 5000.02 Enclosure 14

Air Gap
An interface between two systems that:

- are not connected physically, and
- do not have any logical connection automated (i.e., data is transferred through the interface only manually, under human control).

Source: IETF RFC 4949 Ver 2

Alert
An Internal or external notification that a specific action has been identified within an organization's information systems.

Source: CNSSI 7298 (adapted)

Anti-malware Tools
Tools that help identify, prevent execution, and reverse engineer malware.

Source: CMMC

Anti-spyware Software
A program that specializes in detecting both malware and non-malware forms of spyware.

Source: NIST SP 800-69

Anti-Tamper
Systems engineering activities intended to deter and/or delay exploitation of technologies in a system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Source: DoDI 5200.39 (adapted)

Anti-Virus Software
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Source: NIST SP 800-83

APT (Advanced Persistent Threat)
See Glossary: *Advanced Persistent Threats*

Assessment
Formal process of assessing the implementation and reliable use of issuer controls using various methods of assessment (e.g., interviews, document reviews, observations) that support the assertion that an issuer is reliably meeting the requirements of [FIPS 201-2].

Source: NIST SP 800-79-2

Asset (Organizational Asset)
Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Source: NISTIR 7693, NISTIR 7694

Asset Management
Management of organizational assets. This may include inventory, configuration, destruction, disposal, and updates to organizational assets.

Source: RMM

Asset Owner

A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database.

Source: RMM

Attack Surface

The set of ways in which an attacker can gain unauthorized access to and potentially perform malicious actions on a system. The larger the attack surface, the more opportunities exist to identify flaws and vulnerabilities with an environment.

Source: CMMC

Attribute-Based Access Control (ABAC)

Access control based on attributes associated with and about subjects, objects, targets,initiators, resources, or the environment. An access control rule set defines thecombination of attributes under which an access may take place.

See also Glossary: Identity, Credential, and Access Management (ICAM).

Source: CNSSI 4009

Availability

- Ensuring timely and reliable access to and use of information.
- Timely, reliable access to data and information services for authorized users.

Source: CNSSI 4009

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Source: NIST SP 800-32

Audit Log

A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

Source: CNSSI 4009

Audit Record

An individual entry in an audit log related to an audited event.

Source: NIST SP 800-53 Rev 4

Authentication
A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Source: CNSSI No. 4005, NSA/CSS Manual Number 3-16

Authoritative Data
Data coming from an Authoritative Source.

Source: CMMC

Authoritative Source (trusted source)
An entity that has access to, or verified copies of, accurate information from an issuing source such that a CSP (Credential Service Provider) can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase.

Source: NIST SP 800-63-3

Awareness
A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

Source(s): NIST SP 800-16

Awareness and Training Program
Explains proper rules of behavior for the use of agency information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed. (i.e., NSTISSD 501, NIST SP 800-50)

Source: CNSSI No. 4009

Backup
A copy of files and programs made to facilitate recovery, if necessary.

Source: NIST SP 800-34, CNSSI 4009

Baseline
Hardware, software, databases, and relevant documentation for an information system at a given point in time.

Source: CNSSI 4009

Baseline Configuration
A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Source: NIST SP 800-128

Baseline Security
The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.

Source: NIST SP 800-16

Baselining
Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Source: NIST SP 800-61

Blacklist
A list of discrete entities, such as IP addresses, host names, applications, software libraries, and so forth that have been previously determined to be associated with malicious activity thus requiring access or execution restrictions.

Source: NIST SP 800-114 (adapted), NIST SP 800-94 (adapted), CNSSI 4009 (adapted)

Blacklisting
See Glossary: *Blacklist*

Blacklisting Software
A list of applications (software) and software libraries that are forbidden to execute on an organizational asset.

Source: NIST SP 800-94 (adapted)

Blue Team

1. The group responsible for defending an organization’s use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically, the Blue Team and its supporters must defend against real or simulated attacks:
   - over a significant period of time,
   - in a representative operational context (e.g., as part of an operational exercise), and
   - according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).
2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

Source: CNSSI 4009 (adapted)

Breach

An incident where an adversary has gained access to the internal network of an organization or an organizationally owned asset in a manner that breaks the organizational policy for accessing cyber assets and results in the loss of information, data, or asset. A breach usually consists of the loss of an asset due to the gained access.

Source: CMMC

Capability

Capabilities are achievements to ensure cybersecurity objectives are met within each domain. Capabilities are met through the employment of practices and processes. Each domain is comprised of a set of capabilities.

Source: CMMC

Change Control (Change Management)

Process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.

Source: NIST SP 800-128, CNSSI 4009

Cipher

- Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.
- Series of transformations that converts plaintext to ciphertext using the Cipher Key.

Source: FIPS PUB 197

Ciphertext

Data in its encrypted form.

Source: NIST SP 800-57 Part 1 Rev 3

Compliance

- Verification that the planned cybersecurity of the system is being properly and effectively implemented and operated, usually through the use of assessments / audits.

Source: CMMC

Condition

- The state of something with regard to its appearance, quality, or working order.
- Have a significant influence on or determine (the manner or outcome of something).

Source: Oxford Dictionary

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: 44 U. S. Code Sec 3542

Configuration Item

An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.

Source: NIST SP 800-53 Rev 4

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Source: NIST SP 800-53 Rev 4

Consequence

Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.

Source: NIST SP 800-160

Context Aware
The ability of a system or system component to gather information about its environment at any given time and adapt behaviors accordingly. Contextual or context-aware computing uses software and hardware to automatically collect and analyze data to guide responses.

Source: CMMC

Continuity of Operations
Establish thorough plans, procedures, and technical measures the ability for a system to be recovered as quickly and effectively as possible following a service disruption.

Source: NIST SP 800-34 Rev 1 (adapted)

Control
The methods, policies, and procedures—manual or automated—used by an organization to safeguard and protect assets, promote efficiency, or adhere to standards. A measure that is modifying risk.

(Note: controls include any process, policy, device, practice, or other actions which modify risk.)

Source: NISTIR 8053 (adapted)

Controlled Unclassified Information (CUI)
See Glossary: *CUI*

CUI (Controlled Unclassified Information)
Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Source: E.O. 13556 (adapted)

Custodian
See Glossary: *Asset Custodian*

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: NSPD-54/HSPD-23

Defense Industrial Base (DIB)
The worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Source: DHS CISA

Defined Process
A managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to organizational process assets.

Source: RMM

Dependency
When an entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization.

Source: RMM (adapted)

Demilitarized Zone
Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Source: CNSSI 4009-201

DIB (Defense Industrial Base)
See Glossary: *Defense Industrial Base*

DMZ
See Glossary: *Demilitarized Zone*

Document
Information that is written, printed, or in electronic form that serves as evidence for practices, capabilities, procedures, maturity or processes performed by an organization.

Source: CMMC

Domain
Domains are sets of capabilities that are based on cybersecurity best practices. There are 17 domains within CMMC. Each domain is assessed for practice and process maturity across five defined levels.

Source: CMMC Team

Encryption
The process of changing plaintext into cipher text.

Source: NISTIR 7621 Rev 1, CNSSI 4009

Encryption Policies
Policies that manage the use, storage, disposal, and protection of cryptographic keys used to protect organization data and communications.

Source: RMM

Enterprise

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Source: CNSSI 4009

Enterprise Architecture

The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Source: CNSSI 4009

Establish and Maintain

Whenever "establish and maintain" (or "established and maintained") is used as a phrase, it refers not only to the development and maintenance of the object of the practice (such as a policy) but to the documentation of the object and observable usage of the object. For example, "Formal agreements with external entities are established and maintained" means that not only are the agreements formulated, but they also are documented, have assigned ownership, and are maintained relative to corrective actions, changes in requirements, or improvements.

Source: RMM

Event

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

See Glossary: *Incident*

Source: CNSSI 4009

Event Correlation

Finding relationships between two or more events.

Source: NIST SP 800-92

Exercise

A simulation of an emergency designed to validate the viability of one or more aspects of an information technology plan.

Source: NIST SP 800-84

Facility
Physical means or equipment for facilitating the performance of an action, e.g., buildings, instruments, tools.

Source: NIST SP 800-160

FCI (Federal Contract Information)
Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Source: 48 CFR § 52.204-21

Federated Trust
Trust established within a federation or organization, enabling each of the mutually trusting realms to share and use trust information (e.g., credentials) obtained from any of the other mutually trusting realms. This trust can be established across computer systems and networks architectures.

Source: NIST SP 800-95

Federation
A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.

Source: NIST SP 800-95

Firewall
A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Source: NIST SP 800-41 Rev 1

High-value Assets
Assets, organization information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the organization's interests, relations, economy, or to the employee or stockholder confidence, civil liberties, or health and safety of the organization's people. HVAs may contain sensitive controls, instructions, data used in critical organization operations, or unique collections of data (by size or content), or support an organization's mission essential functions, making them of specific value to criminal, politically motivated, or state sponsored actor for either direct exploitation or to cause a loss of confidence in the organization.

Source: OMB M-17-09 (adapted)

High-value Services
Services built upon High-value Assets which the success of the organization's mission depends.

Source: CMMC

ICAM

See Glossary: *Identity, Credential, and Access Management*

Identity

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. Note: This also encompasses non-person entities (NPEs).

Source: NIST SP 800-161, NISTIR 7622, CNSSI 4009

Identity-Based Access Control (IBAC)

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Source: RMM

Identity, Credential, and Access Management (ICAM)

Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an organization's resources.

See also Glossary: *Attribute-Based Access Control (ABAC)*

Source: CNSSI 4009 (adapted)

Identity Management System

Identity management system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.

Source: NISTIR 8149

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: NIST SP 800-171 Rev 1

Incident Response

A capability set up for the purpose of assisting in responding to computer security-related incidents

Source: NIST SP 800-61

Incident Stakeholder

A person or organization with a vested interest in the management of an incident throughout its life cycle.

Source: RMM

Information Asset Owner
See Glossary: *Asset Owner*

Insider
Any person with authorized access to any organization or United States Government resource to include personnel, facilities, information, equipment, networks, or systems.

Source: CNSSD No. 504

Insider Threat
The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the organization or the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

Source: CNSSD No. 504 (adapted)

Insider Threat Program
A coordinated collection of capabilities authorized by the Department/Agency (D/A) that is organized to deter, detect, and mitigate the unauthorized disclosure of sensitive information.

Source: CNSSD No. 504

Institutionalization
The action of establishing something as a convention or norm in an organization or culture.

Source: Oxford Dictionary

Integrity
The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Source: NIST SP 800-33

Inventory
The physical or virtual verification of the presence of each organizational asset.

Source: CNSSI No. 4005 (adapted)

Least Privilege
A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.

Source: NIST SP 800-57 Part 2

Life Cycle
Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

Source: NIST SP 800-161

Maintenance
Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Source: NIST SP 800-82 Rev 2

Malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware).

Source: NIST SP 800-82 Rev 2

Maturity Model
A maturity model is a set of characteristics, attributes, or indicators that represent progression in a particular domain. A maturity model allows an organization or industry to have its practices, processes, and methods evaluated against a clear set of requirements (such as activities or processes) that define specific maturity levels. At any given maturity level, an organization is expected to exhibit the capabilities of that level. A tool that helps assess the current effectiveness of an organization, and supports determining what capabilities they need in order to obtain the next level of maturity in order to continue progression up the levels of the model.

Source: RMM

Media
Physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, Large-scale integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Source: FIPS PUB 200

Media Sanitization
The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Source: NIST SP 800-88 Rev 1

Mobile Code
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

Source: NIST SP 800-53, NIST SP 800-18, CNSSI 4009

Mobile Device
A portable computing device that:

- has a small form factor such that it can easily be carried by a single individual;
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information);
- possesses local, non-removable data storage; and
- is powered-on for extended periods of time with a self-contained power source.

Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device.

See Glossary: *Portable Storage Device*

Source: NIST SP 800-53 Rev 4

Multifactor Authentication
Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).

See also Glossary: *Authenticator*

Source: NIST SP 800-53 Rev 4

Operational Resilience
The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

Source: CNSSI 4009

Organization
An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).

See Glossary: E*nterprise*

Source: NIST SP 800-37 Rev 1

Organization Seeking Certification (OSC)
The company that is going through the CMMC assessment process to receive a level of certification for a given environment.

Source: CMMC

OSC (Organization Seeking Certification)
See Glossary: *Organization Seeking Certification*

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Source: NIST SP 800-123

Penetration Testing (Pentesting)
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Source: NIST SP 800-115

Pentesting (Penetration Testing)
See Glossary: *Penetration Testing*

Periodically
Organizationally defined regularly occurring intervals, with a timeframe not to exceed one year.

Source: Oxford Dictionary (adapted)

Personally Identifiable Information
Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Source: NIST SP 800-53 Rev 4

PII (Personally Identifiable Information)
See Glossary: *Personally Identifiable Information*

Portable Storage Device
A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).

Source: NIST SP 800-171 Rev 1

Practice
A specific technical activity or activities that are required and performed to achieve a specific level of cybersecurity maturity for a given capability within a domain.

Source: CMMC

Privilege
A right granted to an individual, a program, or a process.

Source: CNSSI 4009, NIST SP 800-12 Rev 1

Process
A specific procedural activity that is required and performed to achieve a capability level. Processes detail maturity of institutionalization of the practices.

Source: CMMC

Proxy
An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.

Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hypertext transfer protocol (HTTP/HTTPS) proxy used for Web access.

Source: CNSSI 4009 (adapted)

Recovery
Actions necessary to restore data files of an information system and computational capability after a system failure.

Source: CNSSI 4009

Red Team
A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Source: CNSSI 4009

Regularly
On a regular basis: at regular intervals.

Source: Oxford Dictionary

Removable Media
Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid-State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

See Glossary: *Portable Storage Device*

Source: CNSSI 4009

Report
An oral or written description of something, such as an event or situation.

Source: NYSSCPA

Reporting
The final phase of the computer and network forensic process, which involves reporting the results of the analysis; this may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

Source: NIST SP 800-86

Residual Risk
Portion of risk remaining after security measures have been applied.

Source: NIST SP 800-33 (adapted)

Resilience
The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Source: PPD 21

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

- the adverse impacts that would arise if the circumstance or event occurs; and
- the likelihood of occurrence

System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Source: FIPS 200 (adapted)

Risk Analysis
The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Source: NIST SP 800-27

Risk Assessment

- The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
- Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Source: NIST SP 800-171 Rev 1

Risk Management
The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes:

- establishing the context for risk-related activities;
- assessing risk;
- responding to risk once determined; and
- monitoring risk over time

Source: CNSSI 4009

Risk Mitigation
Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Source: CNSSI 4009

Risk Mitigation Plan
A strategy for mitigating risk that seeks to minimize the risk to an acceptable level.

Source: RMM

Risk Tolerance
The level of risk an entity is willing to assume in order to achieve a potential desired result.

Source: CNSSI 4009

Root-cause Analysis
An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions.

Source: RMM

Safeguards
The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Source: FIPS PUB 200

Sandboxing
A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

Source: CNSSI 4009

Scanning
Sending packets or requests to another system to gain knowledge about the asset, processes, services, and operations.

Source: CNSSI 4009 (adapted)

SCRM (Supply Chain Risk Management)
See Glossary: *Supply Chain Risk Management*

Security Assessment
See Glossary: *Security Control Assessment*

Security Control Assessment
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for a system or organization.

Source: CNSSI 4009 (adapted)

Security Operations Center
A centralized function within an organization utilizing people, processes, and technologies to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Source: CMMC

Security Policy
Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions “what” and “why” without dealing with “how.” Policies are normally stated in terms that are technology-independent.

Source: NIST SP 800-82 Rev 2

Security Practice Assessment
See Glossary: *Security Control Assessment*

Sensitive Information
Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act).

Source: NIST SP 800-53 Rev 4 (adapted)

Service Continuity Plan
A service-specific plan for sustaining services and associated assets under degraded conditions.

Source: RMM

Situational Awareness
Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Source: CNSSI 4009

SOC
See Glossary: *Security Operations Center*

Split Tunneling
The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.

Source: NIST SP 800-171 Rev 1

Spyware
Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Source: CNSSI 4009, NIST SP 800-128, NIST SP 800-53 Rev 4

Standards
A document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

Source: NISTIR 8074 Vol. 2

Standard Process
An operational definition of the basic process that guides the establishment of a common process in an organization. A standard process describes the fundamental process elements that are expected to be incorporated into any defined process. It also describes relationships (e.g., ordering, interfaces) among these process elements.

See Glossary: *Defined Process*

Source: RMM

Subnetwork
A subordinate part of an organization's enterprise network.

Source: CMMC

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Source: NIST SP 800-53, CNSSI 4009

Supply Chain Attack
Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

Source: CNSSI 4009

Supply Chain Risk Management (SCRM)
A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Source: CNSSD No. 505

Sustain
Maintain a desired operational state.

Source: RMM

System
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

Source: FIPS 200, FIPS 199, CNSSI 4009

System Assets
Any software, hardware (IT, OT, IoT), data, administrative, physical, communications, or personnel resource within an information system.

Source: CNSSI 4009

System Integrity
The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Source: NIST SP 800-27

System Security Plan
The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

Source: CNSSI 4009

Tampering
An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.

Source: DHS Information Technology Sector Baseline Risk Assessment (adapted)

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Source: NIST SP 800-30 Rev 1

Threat Actor
An individual or a group posing a threat.

Source: NIST SP 800-150

Threat Intelligence
Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Source: NIST SP 800-150

Threat Monitoring
Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

Source: CNSSI 4009

Thumb Drive
Removable storage device that utilizes the USB port of a system for data transfer, and the device is relatively the size of a human thumb.

Source: CMMC

Trigger
A set of logic statements to be applied to a data stream that produces an event when an anomalous incident or behavior occurs.

Source - CNSSD No. 504 (adapted)

Trojan Horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Source: CNSSI 4009

Tunneling
Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Source: CNSSI 4009

Unauthorized Access
Any access that violates the stated security policy.

Source: CNSSI 4009

User
Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

Source: NIST SP 800-53, NIST SP 800-18, CNSSI 4009

Virus
A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

See Glossary: *Malicious Code*

Source: CNSSI 4009

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Source: NIST SP 800-30 Rev 1

Vulnerability Assessment
Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Source: CNSSI 4009

Vulnerability Management
An Information Security Continuous Monitoring (ISCM) capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

Source: NISTIR 8011 Vol. 1

Web Proxy
See Glossary: *Proxy*

Whitelist

- An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition.
- An implementation of a default deny-all or allow-by-exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.

Source: CNSSI No. 1011

APPENDIX D: ACRONYM LIST

Below is a list of acronyms used in the CMMC Model Version 0.6.

AA	Audit and Accountability
AC	Access Control
ACSC	Australian Cyber Security Centre
AIA	Aerospace Industries Association
AM	Asset Management
APT	Advanced Persistent Threat
AT	Awareness and Training
AU	Australia
C###	Capability number ###
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CIS	Center for Internet Security
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CNSSI	Committee on National Security Systems Instructions
CSF	Cybersecurity Framework
CSP	Credential Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DNS	Domain Name System
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
IDA	Identification and Authentication
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISCM	Information Security Continuous Monitoring
ITIL	Information Technology Infrastructure Library
L#	Level number #
MA	Maintenance
ML	Maturity Level
ML#	Maturity Level number #
MP	Media Protection

N/A	Not applicable
NAS	National Aerospace Standard
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OUSD A&S	Office of the Under Secretary of Defense for Acquisition and Sustainment
P1###	Practice number ###
PP	Physical Protection
PS	Personnel Security
PUB	Publication
RE	Recovery
Rev	Revision
RM	Risk Management
RMM	Risk Management Model
SA	Situational Awareness
SAS	Security Assessment
SCP	System & Communications Protections
SII	System and Information Integrity
SP	Special Publication
TTP	Tactics, techniques, and procedures
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
VoIP	Voice over Internet Protocol
Vol	Volume