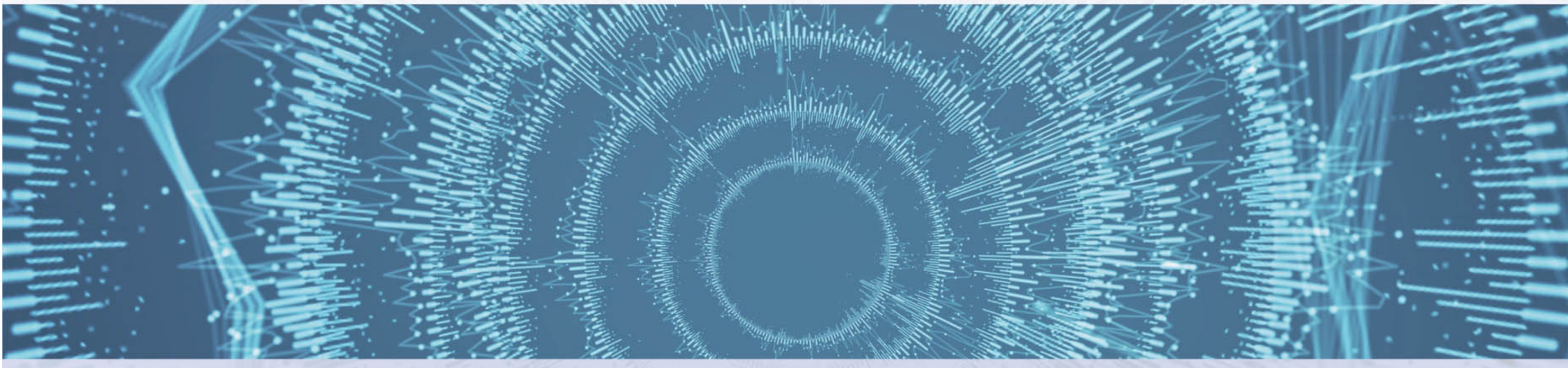
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



DRAFT
Version 0.7
December 6, 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.

[DISTRIBUTION STATEMENT A] Approved for public release.

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 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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 rev 1, Draft NIST SP 800-171B, the United Kingdom's Cyber Essentials, and Australia's Essential Eight [11,12,47,4]. 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 information flow down to subcontractors in a multi-tier supply chain. With respect to implementation, a DIB contractor may meet a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s).

CMMC Versions 0.4 and 0.6 were released for public review in September and November 2019, respectively. CMMC Version 0.7 includes Level 4-5 practices and modifies some maturity processes and Level 1-3 practices.

The DoD is releasing this draft version to support the public's continued review of the draft model in preparation for the release of the CMMC Model Version 1.0 at the end of January 2020. Section 2 describes the model framework, including levels, capability domains, and processes. Section 3 provides instructions on how to read the model. Appendix A presents the latest version of the CMMC Model. Appendices B, C, and D present the practice clarifications for CMMC Levels 1-3, respectively. This document also provides key references, a glossary of terms, and a list of acronyms.

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 mature processes as required for the given CMMC level.

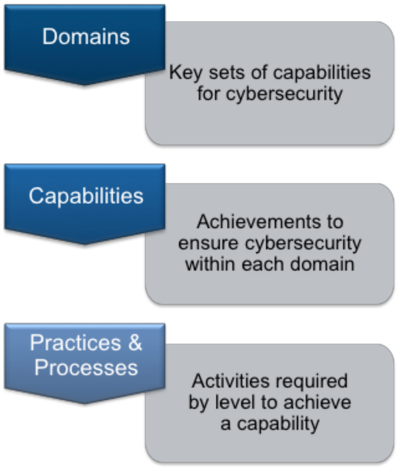

Domains
Key sets of capabilities for cybersecurity
Capabilities
Achievements to ensure cybersecurity within each domain
Practices & Processes
Activities required by level to achieve a capability

Figure 1. CMMC Model Framework

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 Level 5 (advance/progressive). 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.

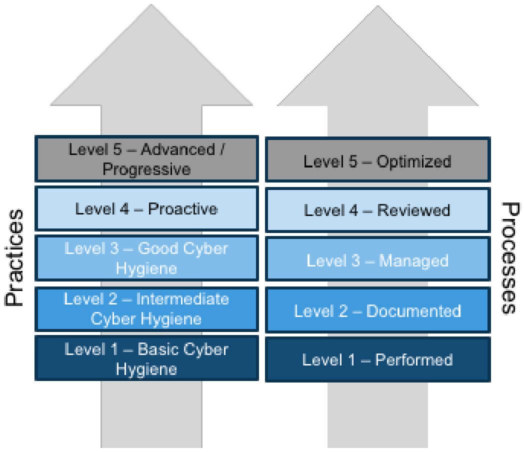


Figure 2. CMMC Level Descriptions

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 processes.

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). Note that organizations subject to DFARS clause 252.204-7012 will have to meet additional requirements such as incident reporting.

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

2.1.4 Level 4

At CMMC Level 4, 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, a CMMC Level 4 organization is expected to review and document activities for effectiveness and inform high-level management of any issues.

2.1.5 Level 5

At CMMC Level 5, an organization has an advanced or progressive cybersecurity program with a demonstrated ability to optimize their cybersecurity capabilities. The organization has the capability to optimize their cybersecurity capabilities in an effort to repel APTs.

For process maturity, a CMMC Level 5 organization is expected to ensure that process implementation has been standardized across the organization.

2.1.6 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 defined 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	N/A	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 for effectiveness and management is informed of any issues	Activities are standardized across all applicable organizational units and identified improvements are shared

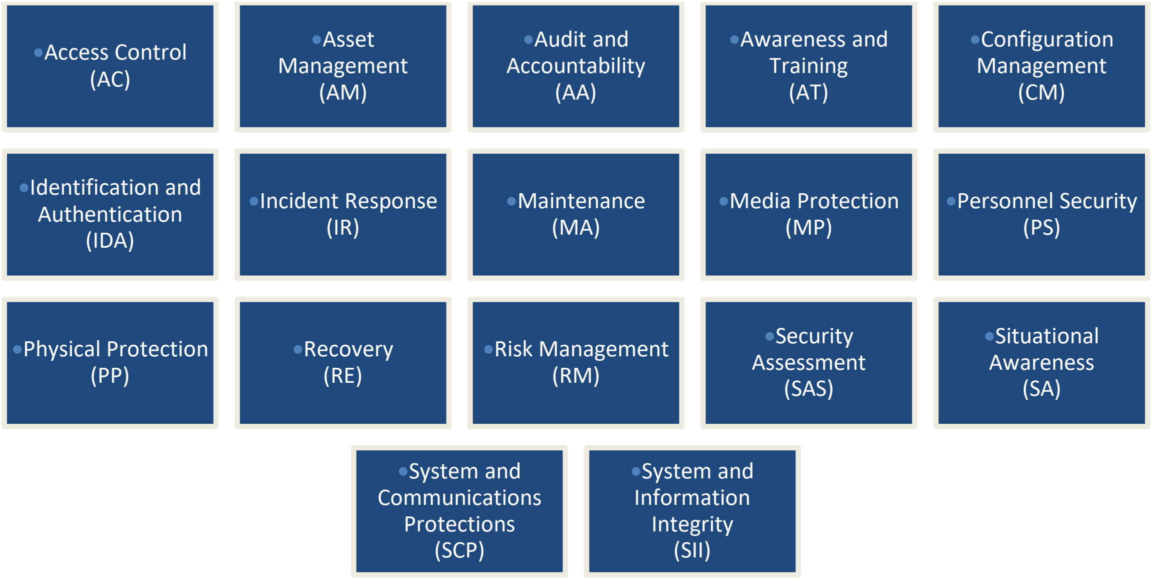
Note that adherence to CMMC processes and practices is cumulative. Once a practice is introduced in a level, it is a required practice for all levels above as well. For an organization to achieve Level 3, all the practices and processes defined in Levels 1, 2, and 3 must be achieved. Similarly, to achieve 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 achieves Level 3 on practice implementation and Level 2 on process institutionalization will be certified at CMMC Level 2. Because the

CMMC model is cumulative, an organization seeking to achieve CMMC Level 3 or higher must implement the practices in Levels 1 and 2 for CUI (in addition to FCI).

2.2 CMMC DOMAINS

The CMMC model consists of 17 domains. The majority of these CMMC domains originated from the Federal Information Processing Standards (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 1-5 of the model, including these practices. More detailed domain definitions are provided in the Appendix F 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
	Manage asset inventory
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
	Manage information security continuity
Risk Management	Identify and evaluate risk
	Manage risk
	Manage supply chain 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 within an organization. Table 3 lists the maturity processes expected to be performed by organizations at each of the five CMMC Levels. 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)

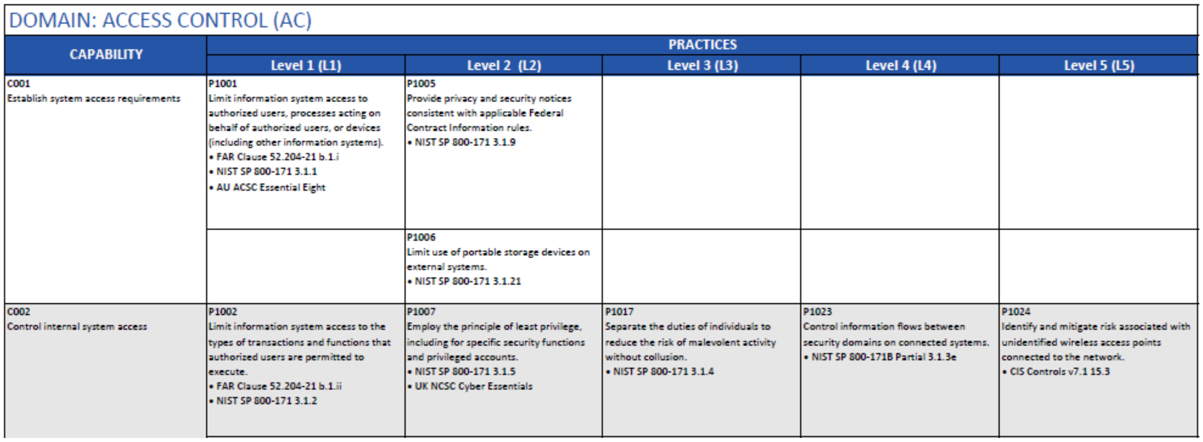
Process Maturity Level	**Processes**
ML 1: Performed	*There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.*
ML 2: Documented	1. Establish a policy that includes [DOMAIN NAME]. 2. Establish practices to implement 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 to meet the plan for [DOMAIN NAME] activities.
ML 4: Reviewed	1. Review and measure [DOMAIN NAME] activities for effectiveness. 2. Review the status and results of [DOMAIN NAME] activities with higher level management and resolve issues.
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 0.7 represents the current iteration in the development of the model.

Figure 4 provides an excerpt of the Version 0.7 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 3-5 for the first capability. As a result, the Level 3-5 cells are blank, but the practices in Level 1 and 2 are still required to achieve Level 3. At the same time, the second capability has required practices at each level. In addition, some levels may have more than one practice per capability. Using the same example, for the first capability Level 2 contains two practices that must be satisfied, in addition to the Level 1 practice, to achieve Level 2 for this capability.



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	P1023 Control information flows between security domains on connected systems. • NIST SP 800-171B Partial 3.1.3e	P1024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CIS Controls v7.1 15.3

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 and serve to provide additional information. 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 4 provides counts of the number of practices derived from key references. Some security requirements from some of the references have not been included based on feedback regarding implementation challenges and costs.

Table 4. CMMC Model Version 0.7 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	55	-	48	-
Level 3	59	-	45	-
Level 4	26	-	-	13
Level 5	16	-	-	5
N/A - Excluded	-	-	-	15
Total	**173**	**15**	**110**	**33**

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). https://eugdpr.org/

APPENDIX A.

CMMC Model Version 0.7
5 December 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.

DM19-0824

Clean Format

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	P1023 Control information flows between security domains on connected systems. • NIST SP 800-171B Partial 3.1.3e	P1024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CIS Controls v7.1 15.3
		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	P1025 Periodically review and update CUI program access permissions. • CMMC	
		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	P1012 Protect wireless access using authentication and encryption. • NIST SP 800-171 3.1.17		
		P1011 Authorize wireless access prior to allowing such connections. • NIST SP 800-171 3.1.16	P1020 Control connection of mobile devices. • NIST SP 800-171 3.1.18 • UK NCSC Cyber Essentials		

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C003 Control remote system access		P1013 Monitor and control remote access sessions. • NIST SP 800-171 3.1.12	P1014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. • NIST SP 800-171 3.1.13	P1032 Restrict remote network access based on organizational defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role. • CMMC	
		P1015 Route remote access via managed access control points. • NIST SP 800-171 3.1.14	P1021 Authorize remote execution of privileged commands and remote access to security-relevant information. • NIST SP 800-171 3.1.15		
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		
C006 Manage asset inventory				P1226 Employ automated capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory. • CMMC modification of NIST SP 800-171B 3.4.3e	

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	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		P1055 Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging. • 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	P1053 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally-defined suspicious activity. • CMMC	
			P1052 Provide audit record reduction and report generation to support on-demand analysis and reporting. • NIST SP 800-171 3.3.6	P1054 Review audit information for broad activity in addition to per-machine activity. • CMMC	

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	P1059 Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat. • NIST SP 800-171B 3.2.1e	
				P1060 Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training. • CMMC modification of NIST SP 800-171B 3.2.2e	
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	P1073 Employ application whitelisting and an application vetting process for systems identified by the organization. • CMMC modfication of NIST SP 800-171 3.4.8 • CIS Controls v7.1 2.7, 2.8, and 2.9	P1074 Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software as defined by the organization. • CMMC modification of NIST SP 800-171B 3.14.1e
		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		P1100 Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution. • CMMC	P1106 In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data. • CMMC
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	P1101 Establish and maintain a security operations center during relevant business hours with on-call response after hours. • NIST SP 800-171B Partial 3.6.1e	P1102 Use a combination of manual and automated, real-time responses to anomalous activities that matches incident patterns. • CMMC
					P1107 Establish and maintain a security operation center that facilitates a 24/7 response capability. • CMMC modification of NIST SP 800-171B 3.6.1e
					P1108 Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours. • CMMC modification of NIST SP 800-171B 3.6.2e
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		P1110 Perform unannounced operational exercises to demonstrate technical and procedural responses. • CMMC

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			P1122 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, as organizationally-defined, 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			
C030 Manage information security continuity					P1140 Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements. • ISO/IEC 27001 A.17.2.1 and A.17.1.2

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. • NIST CSF v1.1 ID.RA • CERT RMM v1.2 RISK:SG3 and SG4.SP3	P1149 Catalog and periodically update threat profiles and adversary TTPs. • NIST CSF v1.1 DE.AE-2	
		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		P1150 Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. • NIST SP 800-171B 3.11.1e • NIST CSF v1.1 ID.RA-2 and ID.RA-3	
				P1151 Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizational-defined boundaries. • CIS Controls v7.1 12.2	
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. • NIST CSF v1.1 ID.RA-6 • CERT RMM v1.2 RISK:SG5.SP1		P1152 Utilize an exception process for non-whitelisted software that includes mitigation techniques. • CMMC
			P1147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. • CMMC		P1155 Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence. • CMMC modification of NIST SP 800-171B 3.11.5e • CERT RMM v1.2 RISK:SG6.SP1
C033 Manage supply chain risk				P1148 Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain. • CMMC modification of NIST SP 800-171B 3.11.7e	

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		P1163 Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement. • NIST CSF v1.1 ID.RM-1, RS.IM-1, RS.IM-2, RC.IM-1, and RC.IM-2	
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	P1164 Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts. • CMMC modification of NIST SP 800-171B 3.12.1e	
		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		P1227 Periodically perform red teaming against defensive capabilities. • CMMC	
C036 Perform code reviews			P1162 Employ code reviews of enterprise software that has been developed internally 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	P1171 Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls. • NIST SP 800-171B 3.11.2e • NIST CSF v1.1 DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM.7, and DE.CM-8	
				P1173 Design network and system security capabilities to leverage, integrate, and share indicators of compromise. • 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		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	P1177 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. • NIST SP 800-171 3.13.11	P1197 Employ physical and logical isolation techniques in the system and security architecture and/or and where deemed appropriate by the organization. • CMMC modification of NIST SP 800-171B 3.13.4e	P1198 Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizational-defined boundaries. • CIS Controls v7.1 12.5
		P1179 Use encrypted sessions for the management of network devices. • CIS Controls v7.1 11.5	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	P1228 Separate administration of organizationally defined high value critical network infrastructure components and servers from production networks (e.g., through out-of-band networks. • CMMC modification of NIST SP 800-171 3.13.2	P1230 Enforce port and protocol compliance. • CMMC
			P1181 Separate user functionality from system management functionality. • NIST SP 800-171 3.13.3 • AU ACSC Essential Eight		
			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		

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
			P1187 Establish and manage cryptographic keys for cryptography employed in organizational systems. • NIST SP 800-171 3.13.10		
			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	P1199 Utilize threat intelligence to proactively block DNS requests from reaching malicious domains. • CMMC	P1208 Employ tailored boundary protections in addition to commercially available solutions. • CMMC
	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 externally-owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter). • CMMC	P1202 Employ mechanisms to sandbox and/or analyze executable code and scripts traversing Internet network boundaries or other organizational-defined boundaries. • CMMC	
				P1229 Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization. • CMMC • CIS Controls v7.1 7.4	

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		P1221 Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting. • NIST SP 800-171B 3.14.6e	
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				P1222 Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions. • CMMC
	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		P1223 Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior. • NIST SP 800-171B 3.14.2e
		P1217 Identify unauthorized use of organizational systems. • NIST SP 800-171 3.14.7			
C044 Implement advanced email protections			P1219 Implement email protections such as DNS or asymmetric cryptography. • CMMC		
			P1220 Utilize sandboxing to detect or block potentially malicious email. • 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.	MP006 Review and measure [DOMAIN NAME] activities for effectiveness.	MP008 Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units.
		MP002 Establish practices to implement the [DOMAIN NAME] policy.	MP005 Provide adequate resources to meet the plan for [DOMAIN NAME] activities.	MP007 Review the status and results of [DOMAIN NAME] activities with higher level management and resolve issues.	MP009 Share identified improvements to [DOMAIN NAME] activities across the organization.
		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

- 48 CFR 52.204-21 b.1.i.i
- NIST SP 800-171 3.1.1

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

- 48 CFR 52.204-21 b.1.ii
- NIST SP 800-171 3.1.2

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

- 48 CFR 52.204-21 b.1.iii
- NIST SP 800-171 3.1.20

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

- 48 CFR 52.204-21 b.1.iv
- NIST SP 800-171 3.1.22

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

- 48 CFR 52.204-21 b.1.v
- NIST SP 800-171 3.5.1

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

- 48 CFR 52.204-21 b.1.vi
- NIST SP 800-171r1 3.5.2

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

- 48 CFR 52.204-21 b.1.vii
- NIST SP 800-171 3.8.3

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

- 48 CFR 52.204-21 b.1.viii
- NIST SP 800-171 3.10.1
- CERT RMM v1.2 KIM:SG4.SP2

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

- 48 CFR 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.3

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

- 48 CFR 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.4

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

- 48 CFR 52.204-21 Partial b.1.ix
- NIST SP 800-171 3.10.5
- CERT RMM v1.2 KIM:SG4.SP2

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

- 48 CFR 52.204-21 b.1.x
- NIST SP 800-171 3.13.1

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

- 48 CFR 52.204-21 b.1.xi
- NIST SP 800-171 3.13.5

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

- 48 CFR 52.204-21 b.1.xii
- NIST SP 800-171 3.14.1

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

- 48 CFR 52.204-21 b.1.xiii
- NIST SP 800-171 3.14.2

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

- 48 CFR 52.204-21 b.1.xiv
- NIST SP 800-171 3.14.4

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

- 48 CFR 52.204-21 b.1.xv
- NIST SP 800-171 3.14.5

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. CMMC LEVEL 2 DISCUSSION AND CLARIFICATION

Introduction

This draft provides discussion and clarifications for the CMMC Level 2 practices.

Please note that the clarification examples are intended only to help explain the practices and do not represent guidance.

Access Control (AC) P1005: Provide privacy and security notices consistent with applicable Federal Contract Information rules.

REFERENCES

- NIST SP 800-171 3.1.9

DISCUSSION [DRAFT NIST SP 800-171R2]

System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

CLARIFICATION

Every system has legal information about user privacy and security. A system use notification banner displays the legal requirements of using the systems. Users are required to click to agree to the displayed requirements of using the system each time they logon to the machine. You can use this implicit agreement in the civil and/or criminal prosecution of an attacker that violates the terms.

Discuss legal notification requirements with your organization’s legal counsel. This will ensure that they meet all applicable requirements. You should inform the user that:

- you may monitor, record, and subject to audit any information system usage
- you prohibit unauthorized use of the information system
- you may subject unauthorized use to criminal and civil penalties
- use of the information system indicates consent to monitoring and recording

Example

You are setting up IT equipment for your organization. You have worked with legal counsel to draft a notification. The system displays the required security and privacy information when anyone logs on to your organization’s machines. You ensure that this notification displays to all users of all of the organization’s machines.

Access Control (AC) P1006: Limit use of portable storage devices on external systems.

REFERENCES

- NIST SP 800-171 3.1.21

DISCUSSION [DRAFT NIST SP 800-171R2]

Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. 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 CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI 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

A portable storage device is a system component that you can insert and remove from a system. You use it to store data or information. Examples of portable storage devices include:

- floppy disks
- compact/digital video disks (CDs/DVDs)
- flash/thumb drives
- external hard disk drives
- flash memory cards/drives that contain nonvolatile memory.

You can put this practice in place two ways:

- set up a policy that describes the usage restrictions of these devices; or
- establish technical means, such as configuring devices to work only when connected to a system to which they can authenticate

Example

Your organization has a usage restriction policy. It states that users cannot use portable storage devices in external information systems without management approval.

Access Control (AC) P1007: Employ the principle of least privilege, including for specific security functions and privileged accounts.

REFERENCES

- NIST SP 800-171 3.1.5
- UK NCSC Cyber Essentials

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

CLARIFICATION

You should apply the principle of least privilege to all users and processes on all systems. This means you assign the fewest permissions necessary for the user or process to accomplish their business function. Also, you:

- restrict user access to only the machines and information needed to fulfill job responsibilities
- limit what system configuration settings users can change. You allow only individuals with a business need to change them

Example

As the IT administrator for your organization, you create accounts. You apply the fewest privileges necessary for the user or process to complete their task. This means you assign everyone a basic user role. This prevents a user from modifying system configurations. Also, you assign privileged access only to users and processes that need it, such as IT staff.

Access Control (AC) P1008: Use non-privileged accounts or roles when accessing nonsecurity functions.

REFERENCES

- NIST SP 800-171 3.1.6
- UK NCSC Cyber Essentials

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

CLARIFICATION

A user with a privileged account can perform extra tasks and access more information than a person with a non-privileged account. This means that tasks performed when using the privileged account can have a greater impact on the system. You restrict administrator use of privileged accounts. Only those who perform a function that requires more access have a privileged account. This reduces the risk of unintentional harm to systems and data.

Example

As the IT administrator for your organization, you have two user accounts. One is a non-privileged account, which you use when performing non-privileged duties. These tasks include sending or receiving emails. The other is a privileged account, which you use only when performing administrative functions. Examples include troubleshooting a device or setting up new user accounts.

Access Control (AC) P1009: Limit unsuccessful logon attempts.

REFERENCES

- NIST SP 800-171 3.1.8

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

CLARIFICATION

Consecutive, unsuccessful logon attempts may indicate malicious activity. You can mitigate these types of attacks by limiting the number of unsuccessful logon attempts. There are many ways to do this. Having three consecutive, unsuccessful logon attempts is a common setting. Organizations should set this number at a level that fits their risk profile. Fewer unsuccessful attempts provide higher security.

After the system locks an account, it has several options to unlock it. The most common is to lock the account for a predefined time. After that time, the account unlocks. Another option is to keep the account locked until an administrator unlocks it.

Example

You attempt to log on to your work computer. You mistype your password three times in a row. You call your IT help desk or administrator. The administrator tells you your account is locked. He explains that all passwords lock after three unsuccessful logon attempts. This limits the effectiveness of brute-force and other password attacks. He tells you he can unlock it, or you can wait five minutes and the account will unlock automatically.

Access Control (AC) P1010: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

REFERENCES

- NIST SP 800-171 3.1.10

DISCUSSION [DRAFT NIST SP 800-171R2]

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

CLARIFICATION

You can set session locks on your system. A user can enable the lock. Also, the system can enable it automatically after a preset time, for example, from one to five minutes. Session locks are a quick way to prevent unauthorized use of the systems without having a user log off.

A locked session shows pattern-hiding information on the machine screen. This masks the data on the display.

Example

You are the IT administrator in your organization. You notice that employees leave their offices without locking their computers. Sometimes their screens display sensitive company information. You remind your coworkers to lock their systems when they walk away. You set all machines to lock after five minutes of inactivity.

Access Control (AC) P1011: Authorize wireless access prior to allowing such connections.

REFERENCES

- NIST SP 800-171 3.1.16

DISCUSSION [DRAFT NIST SP 800-171R2]

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

CLARIFICATION

You should base the use of wireless technologies on approved guidelines from management. These guidelines may include:

- the types of devices, such as corporate or privately-owned equipment
- the configuration requirements of the devices
- the authorization requirements before granting such connections

Example

Your company is implementing a wireless network at their headquarters. You work with management to draft policies about the use of the wireless network. You allow only company-approved devices that contain verified security configuration settings. Also, you write usage restrictions to follow for anyone who wants to use the wireless network.

Access Control (AC) P1013: Monitor and control remote access sessions.

REFERENCES

- NIST SP 800-171 3.1.12

DISCUSSION [DRAFT NIST SP 800-171R2]

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

[SP 800-46], [SP 800-77], and [SP 800-113] provide guidance on secure remote access and virtual private networks.

CLARIFICATION

Remote access connections pass through untrusted networks and should therefore not be trusted without proper security controls in place. All remote access should implement approved encryption. This ensures the confidentiality of the data. Check connections to ensure that only authorized users and devices are connecting. Monitoring may include tracking who is accessing the network remotely and what files they are access during the remote session.

Example

You work from remote locations, such as your house or a client site and need access to your company's network. The IT administrator issues you a company laptop with a VPN software installed which is required to connect to the network remotely. After you connect to the VPN, you must accept a privacy notice which states that the company's security department may monitor your connection. They do this through the use of a network-based Intrusion Detection System (IDS). They also review audit logs to see who is connecting remotely and when. Next you see the message "Verifying compliance." This means the system is checking your device to ensure it meets the established requirements to connect. The administrator explains that after your machine connects to the network

Example *(continued)*

using the VPN, you can have confidence that your session is private because your company implements approved encryption.

Access Control (AC) P1014: Route remote access via managed access control points.

REFERENCES

- NIST SP 800-171 3.1.14

DISCUSSION [DRAFT NIST SP 800-171R2]

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

CLARIFICATION

You can limit the number of remote access control points. This reduces the attack surface for organizations. Route all remote access sessions through as few points as possible. This:

- allows for better visibility into the traffic coming into the network
- simplifies network management
- increases the ability to monitor and control the connections

Example

You are the IT administrator for a company with many locations. Several employees at different locations need to connect to the network while working remotely. Each location has its own connection to the internet. You decide to route all remote access through the headquarters location. Each company location has a direct connection to headquarters. So, it makes sense to route remote access traffic through headquarters. All remote traffic comes to one location. You have to monitor the traffic on only one device, rather than one per location. The company will not have to buy as much equipment.

Access Control (AC) P1016: Control the flow of Federal Contract Information in accordance with approved authorizations.

REFERENCES

- NIST SP 800-171 3.1.3

DISCUSSION [DRAFT NIST SP 800-171R2]

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

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies.

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.

In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes:

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

prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

CLARIFICATION

Flow control regulates where and how information can flow. Firewalls and proxy servers can be used to control traffic flow. Typically, organizations will have a firewall between the internal network and the internet. Often multiple firewalls are used inside a network to create zones to separate sensitive data, business units or user groups. Proxy servers can be used to break the connection between multiple networks. All traffic entering or leaving a network is intercepted by the proxy, preventing direct access between networks. This can have security and performance benefits. Additionally, organizations should ensure that all sensitive information is encrypted before being transmitted over the internet.

Example

You configure a proxy device on your company's network. Your goal is to better mask and protect the devices inside your network. After you configure the device, information does not flow directly from the internal network to the internet. The proxy system intercepts the traffic. Then, the proxy analyzes it to determine if it is legitimate. If it is, the system allows it on the network and sends it to its destination.

Audit & Accountability (A&A) 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.

REFERENCES

- NIST SP 800-171 3.3.2

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of VoIP.

CLARIFICATION

You need to capture information in audit logs. This ensures that you can trace the actions you audit to a specific user. This may include capturing information from users, including:

- user ID's
- source and destination addresses
- time stamps

Such information helps track actions to an individual.

Example

You are the IT administrator for your organization. You want to ensure that you can trace all remote access sessions to a specific user. You configure the VPN device to capture the following information for all remote access connections:

- source and destination IP address
- user ID
- machine name
- time stamp
- user actions during the remote session

This lets you trace these actions to a specific user.

Audit & Accountability (A&A) 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.

REFERENCES

- NIST SP 800-171 3.3.1

DISCUSSION [DRAFT NIST SP 800-171R2]

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making. [SP 800-92] provides guidance on security log management.

CLARIFICATION

You should ensure that the system creates and retains audit logs. The logs should contain enough information to identify and investigate unlawful or unauthorized system activity. You select the events that require auditing. Also, you determine the information to record in the audit logs about those events.

Example

You set up audit logging capability for your organization. You determine that all systems that contain CUI must have extra detail in the audit logs. Because of this, you configure these systems to log the following information for all user actions:

- time stamps
- source and destination addresses
- user or process identifiers
- event descriptions
- success or fail indications, and filenames

Audit & Accountability (A&A) P1043: Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

REFERENCES

- NIST SP 800-171 3.3.7

DISCUSSION [DRAFT NIST SP 800-171R2]

Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

CLARIFICATION

Some organizations have many machines. It is good practice to setup each machine to synchronize its time with a central time server. This ensures that all machines are recording audit logs using the same time source. This is important when you review audit logs for suspicious activity. You need to review events from multiple machines. This can be a difficult task if the time is not synchronized for all machines. To use the same time source, you can synchronize machines to a network device or directory service. Also, you can configure machines manually to use the same time servers on the internet.

Example

You are setting up several new computers on your company's network. They are not setup on a domain. You update the time settings on each machine to use the same authoritative time server on the internet. So, if you have to review audit logs, all your machines have synchronized time. This helps you investigate a potential incident.

Audit & Accountability (A&A) P1044: Review audit logs

REFERENCES

- CMMC

DISCUSSION [CMMC]

Reviewing audit logs is a control in information security. Organizations have the flexibility to determine which logs and specific events to review. The level of audit log review should be determined based on a risk assessment or similar activity.

CLARIFICATION

You should ensure that your organization reviews its audit logs. The process of reviewing audit logs varies by organization. The intent of this practice is to become familiar with the logs being automatically created on the systems present in your organization and identify key events in the logs that might indicate malicious activity. Logs should be checked regularly, organizations with small environments may be able to do this manually. Larger organizations may need automation to complete this task with success.

Example

You are the administrator for a company with a small IT environment. You know the importance of reviewing audit logs. Every week you log on to the Windows server as an admin user, open the Event Viewer and check for signs that the log files have been altered: Windows event ID 104 – Event Log was Cleared, event ID 1102 – Audit Log was Cleared), event ID 4719 – System audit policy was changed. Look for login and new user created events: Windows event IDs 4624 (failure) and 4625 (success)) and event IDs 4728, 4732 and 4756 – User added to Privileged Group.

Awareness & Training (AT) 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.

REFERENCES

- NIST SP 800-171 3.2.1
- CERT RMM v1.2 OTA:SG1.SP1

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

[SP 800-50] provides guidance on security awareness and training programs.

CLARIFICATION

Awareness training focuses user attention on security. You can use several techniques to do this:

- instructor or online training
- security awareness campaigns
- posters and email advisories and notices to employees

There is an important distinction between awareness training and role-based training. Awareness training provides general security training to influence user behavior. Role-based training focuses on the knowledge, skills, and abilities needed to complete a specific job.

Example

You want to provide information to employees so they can identify phishing emails. To do this, you prepare a presentation that highlights basic traits, including:

- suspicious-looking email address or domain name
- a message that contains an attachment or URL
- a message that is poorly written and often contains obvious misspelled words

You encourage everyone to not click on attachments or links in a suspicious email. You tell employees

Example *(continued)*

to forward such a message immediately to their IT security administrator. You download free security awareness posters to hang in the office. Also, you send regular emails and tips to all employees. This ensures that your message is not forgotten over time.

Awareness & Training (AT) P1057: Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

REFERENCES

- NIST SP 800-171 3.2.2
- CERT RMM v1.2 OTA:SG4.SP1

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

[SP 800-181] provides guidance on role-based information security training in the workplace. [SP 800-161] provides guidance on supply chain risk management.

CLARIFICATION

Training imparts skills and knowledge. It enables staff to perform a specific resilience function. Training programs identify cybersecurity skill gaps within your organization. Then, the programs train users on their specific cybersecurity roles and responsibilities.

There is an important distinction between awareness training and role-based training. Awareness training provides general security training to influence user behavior. Role-based training focuses on the knowledge, skills, and abilities needed to complete a specific job.

Example

Your company upgraded the firewall to a new device. This device is more advanced than the old machine. Your company identified you as an employee who needs training on the device. This will enable you to use it effectively. Your company considered this when it planned for the upgrade. It made training funds available as part of the upgrade project.

Configuration Management (CM) P1061: Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

REFERENCES

- NIST SP 800-171 3.4.1
- CERT RMM v1.2 KIM:SG5.SP2
- UK NCSC Cyber Essentials

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement establishes and maintains baseline configurations for systems and system components including for system communications and connectivity. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

[SP 800-128] provides guidance on security-focused configuration management.

CLARIFICATION

You should build and configure systems from a known, secure, and approved configuration baseline. This includes:

- documenting the software and configuration settings of a system
- placement within the network
- other specifications as required by the organization

CLARIFICATION *(continued)*

An effective cybersecurity program depends on system and component configuration and management.

Example

You are in charge of upgrading the computer operating systems of your office's 10 machines. You research how to setup and configure a machine with the least functionality and highest security. The setup must allow users to do their tasks. You document this configuration. Then, you apply it to the other nine machines. You understand the baseline configuration of every machine. This helps when you need to install new patches, software, or make changes.

Configuration Management (CM) P1062: Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

REFERENCES

- NIST SP 800-171 3.4.6
- UK NCSC Cyber Essentials

DISCUSSION [DRAFT NIST SP 800-171R2]

Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

CLARIFICATION

You should customize organizational systems. To do this, remove non-essential applications and disable services not needed. Systems come with many unnecessary applications and settings enabled by default. Disable unnecessary software and services. These include unused ports and protocols. Leave only the fewest capabilities necessary for the systems to operate effectively.

Example

You know that systems often include unnecessary software and services enabled by default. You deploy new servers in your organization’s IT environment. Before you do so, you review each system’s role and minimum required capabilities. You remove software that is not needed. You disable unused ports and services. You leave only the fewest capabilities enabled for the system to function in its role.

Configuration Management (CM) P1063: Control and monitor user-installed software.

REFERENCES

- NIST SP 800-171 3.4.9

DISCUSSION [DRAFT NIST SP 800-171R2]

Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved “app stores.” Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

CLARIFICATION

You should limit installed software to items that the organization approved. Users will install software that creates unnecessary risk. This risk applies both to the machine and to the larger operating environment. You should control the software users can install. You should put in place policies and technical controls that can reduce risk to the organization.

Example

You are the IT administrator for your company. A user calls you for help installing a software package. He keeps receiving a message asking for a password. The user receives the message because he does not have permission to install the software. You explain the organization’s policy. It prohibits users from installing software without approval. When you set up workstations for users, you do not provide administrative privileges. You make an exception only if a user needs administrative access to do his job. After the call, you redistribute the policy to all users. Everyone in the organization is aware of the restrictions.

Configuration Management (CM) P1064: Establish and enforce security configuration settings for information technology products employed in organizational systems.

REFERENCES

- NIST SP 800-171 3.4.2
- UK NCSC Cyber Essentials

DISCUSSION [DRAFT NIST SP 800-171R2]

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

[SP 800-70] and [SP 800-128] provide guidance on security configuration settings.

CLARIFICATION

Security-related configuration settings should be customized and included as part of an organization's baseline configurations for all information systems. These configuration settings should satisfy the organization's security requirements and changes or deviations to the security settings should be documented. Organizations should document the Security-related configuration settings and apply them to all systems once tested and approved. The configuration settings should reflect the most

CLARIFICATION *(continued)*

restrictive settings that are appropriate for the system. This ensures that information security is an integral part of an organization’s configuration management process.

Example

You are in charge of establishing baseline configurations for your organization’s systems. As part of this, you document the most restrictive settings that still allow the system to function as required and apply this configuration to all applicable systems. This secure configuration, also known as a system lockdown, blocks unapproved applications from running on the system. The lockdown configuration aligns with your organization’s security requirements.

Configuration Management (CM) P1065: Track, review, approve, or disapprove, and log changes to organizational systems.

REFERENCES

- NIST SP 800-171 3.4.3
- CERT RMM v1.2 KIM:SG5.SP2
- AU ACSC Essential Eight

DISCUSSION [DRAFT NIST SP 800-171R2]

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.

[SP 800-128] provides guidance on configuration change control.

CLARIFICATION

You should track, review, and approve changes before committing to production. Changes to computing environments can create unintended and unforeseen issues. They can affect the security and availability of the systems. Organizations should hold regular meetings about changes. Relevant experts should review and approve proposed changes. They should discuss potential impacts, before the organization puts the changes in place. Relevant items include changes to the physical environment and to the system hosted within it.

Example

Once a month, the management and technical team leads join a change control board meeting. During this meeting, everyone reviews all proposed changes to the environment. This includes changes to the physical and computing environments. The meeting ensures that relevant subject matter experts review changes and propose alternatives where needed.

Configuration Management (CM) P1066: Analyze the security impact of changes prior to implementation.

REFERENCES

- NIST SP 800-171 3.4.4

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

[SP 800-128] provides guidance on configuration change control and security impact analysis.

CLARIFICATION

You should analyze the potential security impact of changes before implementing them. Changes to complex environments can cause unforeseen problems to systems and environments. You should perform an analysis that focuses on the security impact of changes. This can uncover potential problems before you implement the change. By doing so, you can help mitigate unforeseen problems.

Example

Someone requests major changes to the system and environment. You must complete a process with several steps before you can put the change in place. You document a detailed plan. An SME who did not submit the change reviews the plan. That SME tries to identify security-related issues that the change may cause. Then, he documents or corrects the potential issues. Also, he submits the updated change plan to your organization’s change control board.

Identification and Authentication (IDA) P1078: Enforce a minimum password complexity and change of characters when new passwords are created.

REFERENCES

- NIST SP 800-171 3.5.7

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

CLARIFICATION

Password complexity means using different types of characters as well as a specified number of characters. These include numbers, lowercase and uppercase letters, and symbols. Define the lowest level of password complexity required. Enforce this rule for all new passwords.

Example

You are in charge of setting your organization’s password rules. Everyone must use a combination of different types of characters for all new and changed passwords. Also, there is an established number of minimum characters for each password. Characters include numbers, lowercase and uppercase letters, and symbols. These rules help create hard-to-guess passwords, which help to secure your network.

Identification and Authentication (IDA) P1079: Prohibit password reuse for a specified number of generations.

REFERENCES

- NIST SP 800-171 3.5.8

DISCUSSION [DRAFT NIST SP 800-171R2]

Password lifetime restrictions do not apply to temporary passwords.

CLARIFICATION

Individuals may not reuse passwords for a defined period of time and a set number of passwords generated.

Example

You are in charge of setting your organization’s password rules. You define how often individuals can reuse their passwords and the minimum number of password generations before reuse. Using new passwords helps provide increased network security.

Identification and Authentication (IDA) P1080: Allow temporary password use for system logons with an immediate change to a permanent password.

REFERENCES

- NIST SP 800-171 3.5.9

DISCUSSION [DRAFT NIST SP 800-171R2]

Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

CLARIFICATION

Users must change their temporary passwords the first time they log in.

Example

You are in charge of setting temporary passwords for your users. Users must change their temporary passwords to a permanent password the first time they log in. Temporary passwords are less secure than permanent passwords.

Identification and Authentication (IDA) P1081: Store and transmit only cryptographically-protected passwords.

REFERENCES

- NIST SP 800-171 3.5.10

DISCUSSION [DRAFT NIST SP 800-171R2]

Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords. See [NIST Cryptographic Standards and Guidelines].

CLARIFICATION

All passwords must be cryptographically protected in a one-way function for storage and transmission. This type of protection changes passwords into another form, or a hashed password. A one-way transformation makes it nearly impossible to turn the hashed password back into the original password.

Example

You are responsible for managing passwords for your organization. You protect on all passwords with a one-way transformation, or hashing, before storing or transmitting them.

Identification and Authentication (IDA) P1082: Obscure feedback of authentication information.

REFERENCES

- NIST SP 800-171 3.5.11

DISCUSSION [DRAFT NIST SP 800-171R2]

The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

CLARIFICATION

A password is a type of authentication information. When users enter this information, the system displays a symbol, such as an asterisk. This prevents others from seeing the actual characters. The organization should obscure feedback based on a defined policy. For example, smaller devices may briefly show characters before obscuring.

Example

You are in charge of IT for your company. You set up your systems to display a symbol, such as an asterisk, when users enter their passwords into a computer system. For your mobile devices, the password characters are briefly displayed to the user before being obscured. This prevents people from figuring out passwords by looking over someone’s shoulder.

Incident Response (IR) P1092: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recover, and user response activities.

REFERENCES

- NIST SP 800-171r1 3.6.1

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

[SP 800-61] provides guidance on incident handling. [SP 800-86] and [SP 800-101] provide guidance on integrating forensic techniques into incident response. [SP 800-161] provides guidance on supply chain risk management.

CLARIFICATION

Incident handling should include activities that prepare your organization to respond to incidents. These activities may include the following:

- identify people inside and outside your organization you may need to contact during an incident
- establish a way to report incidents, such as an email address or a phone number
- establish a system for tracking incidents
- determine a place and a way to store evidence of an incident

CLARIFICATION *(continued)*

You may need software and hardware to analyze incidents when they occur. You should also consider incident prevention activities as part of your incident-handling capability. The incident handling team provides input for such things as risk assessments and training.

Your organization should detect incidents in different ways. Use indicators to detect incidents. Indicators are things that don't look like what you expect. Examples include:

- alerts from your sensors or antivirus software
- a filename that looks unusual
- a log entry that raises concern

After you detect an incident, you should analyze it to decide what to do. To analyze an incident, you need to know what should be occurring on your network and what should not. This will help you determine when incident may have occurred. It may also help you decide what to do about it. You should also document what you know about the incident. Include all the log entries associated with the incident in your documentation.

Containment of the incident is important. This stops the damage the incident is causing to your network. You should base the containment activities you do off your incident analysis. These activities can include:

- disconnecting a system from the internet
- changing firewall settings to stop an attack

Recovery activities are things to fix that caused the incident. This will help prevent the incident happening again. Recovery activities also include things that fix the affected systems, including:

- restoring back-up data
- reinstalling software

User response activities include:

- performing a lessons-learned analysis
- deciding if you should contact the police
- updating any policy or plans as a result of after incident analysis

Example 1

Your manager asks you to set up your organization's incident-response capability. First, you create an email address to collect information on possible incidents. Next, you draft a contact list of all the people in the organization who need to know when an incident occurs. Then, you write down a procedure for how to submit incidents. This includes what everyone should do when a potential incident is detected or reported. The procedure also explains how to track incidents, from initial creation to closure.

Example 2

You receive an email alert about a possible incident. An employee identified a suspicious email message as a phishing attempt. First, you document the incident in your incident tracking system. Then, you immediately reference your defined procedures for handling incidents. For example, you send an email to your employees alerting them not to open a similar email. You also start collecting information around the reported incident.

Example 3

In response to the suspicious email, you perform a set of actions.

1. You reinstall the software on the machine of the user involved. This means that the individual no longer has an infected machine.
2. You update your phishing protection software. This ensures that it can block the latest phishing attacks.
3. You update your training material to emphasize the threat of phishing emails.

Incident Response (IR) P1093: Detect and report events.

REFERENCES

- CERT RMM v1.2 IMC:SG2.SP1

DISCUSSION [CERT RMM V1.2 IMC:SG2:SP1]

The monitoring, identification, and reporting of events are the foundation for incident identification and commence the incident life cycle. Events potentially affect the productivity of organizational assets and, in turn, associated services. These events must be captured and analyzed so that the organization can determine whether an event will become (or has become) an incident that requires organizational action. The extent to which an organization can identify events improves its ability to manage and control incidents and their potential effects.

CLARIFICATION

Detect events on your network. An event is any observable occurrence on the network. You can detect events several ways, including through:

- observations of breakdowns in processes or loss in productivity
- observations such as alarms and alerts, notification from other organizations
- the results of audits or assessments

After you detect an event, report it to stakeholders who need to act on the event.

Example

You are in charge of IT operations for your company. As part of your role, you should look out for events on your network. You should also be a collection point for your coworkers to send you suspected events. When you discover or receive a report of an event, you should tell the person who will need to act on the detected event.

Incident Response (IR) P1094: Analyze and triage events to support event resolution and incident declaration.

REFERENCES

- CERT RMM v1.2 IMC:SG2.SP4

DISCUSSION [CERT RMM V1.2 IMC:SG2:SP4]

The triage of event reports is an analysis activity that helps the organization to gather additional information for event resolution and to assist in incident declaration, handling, and response. Triage consists of categorizing,

correlating, prioritizing, and analyzing events. Through triage, the organization determines the type and extent of an event (e.g., physical versus technical), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response. Triage also helps the organization to determine if the event needs to be escalated to other organizational or external staff (outside of the incident management staff) for additional analysis and resolution.

Some events will never proceed to incident declaration; the organization determines these events to be inconsequential. For events that the organization deems as low priority or of low impact or consequence, the triage process results in closure of the event and no further actions are performed.

Events that exit the triage process warranting additional attention may be referred to additional analysis processes for resolution or declared as an incident and subsequently referred to incident response processes for resolution. These events may be declared as incidents during triage, through further event analysis, through the application of incident declaration criteria, or during the development of response strategies, depending on the organization’s incident criteria, the nature and timing of the event(s), and the consequences of the event that the organization is currently experiencing or that is imminent.

CLARIFICATION

Analyze events to determine what to do. Categorize, prioritize, or group events to determine how to handle the event. You can take different actions in response to an event:

- declare an incident from the event
- escalate it to someone outside the organization
- close the event because it does not have a large consequence on the organization

Example

You are in charge of IT operations for your company. As part of your role, you are the collection point for events. You should analyze all events to determine what actions to take. Through analysis, you

Example *(continued)*

should determine:

- the type and extent of an event (e.g., physical versus technical)
- whether the event is related to other events (to determine if they are part of a larger issue, problem, or incident)
- in what order events should be addressed

Analysis also helps the organization determine whether to escalate the event to external staff. If so, the external staff can perform analysis and resolution.

Incident Response (IR) P1096: Develop and implement responses to declared incidents according to predefined procedures.

REFERENCES

- CERT RMM V1.2 IMC:SG4.SP2

DISCUSSION [CERT RMM V1.2 IMC:SG4.SP2]

Responding to an organizational incident is often dependent on proper advance planning by the organization in establishing, defining, and staffing an incident management capability.

Responding to an incident describes the actions the organization takes to prevent or contain the impact of an incident on the organization while it is occurring or shortly after it has occurred. The range, scope, and breadth of the organizational response will vary widely depending on the nature of the incident. Incident response may be as simple as notifying users to avoid opening a specific type of email message or as complicated as having to implement service continuity plans that require relocation of services and operations to an off-site provider. The broad range of potential incidents requires the organization to have a broad range of capability in incident response.

CLARIFICATION

Respond to declared incidents. Do this by preventing or containing the impact of an incident while it is occurring or shortly after. The type of response will vary depending on the incident. Response actions might include:

- stopping the damage (e.g., by taking hardware or systems offline)
- communicating to users (e.g. avoid opening a specific type of email message)
- implementing controls (e.g. updating access control lists)

Example

You are in charge of IT operations for your company. In this role, you manage all declared incidents. You have procedures in place for handling different types of declared incidents. For example, when you identify a phishing email incident, you have a process in place. You notify your company about the suspicious email and what to do when you receive it.

Incident Response (IR) P1097: Perform root cause analysis on incidents to determine underlying causes.

REFERENCES

- CERT RMM V1.2 IMC:SG5.SP1

DISCUSSION [CERT RMM V1.2 IMC:SG5.SP1]

Post-incident review is a formal part of the incident closure process. The organization conducts a formal examination of the causes of the incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur.

Post-incident review should include a significant root-cause analysis process. The organization should employ commonly available techniques (such as cause-and-effect diagrams) to perform root-cause analysis as a means of potentially preventing future incidents of similar type and impact. Considerations of other processes that may have caused or aided the incident should be given, particularly as they may exist in processes such as change management and configuration management.

CLARIFICATION

Examine the causes of the event or incident and how your organization responded to it. Look at the administrative, technical, and physical control weaknesses. These may have allowed the incident to occur. Use available practices, such as cause-and-effect diagrams, to perform root-cause analysis. This will prevent future similar incidents. After incidents are resolved, conduct reviews and capture lessons learned. Make improvements based on the outcomes of these activities, such as updating plans or controls.

Example

You are in charge of IT operations for your company. As part of your role, you manage incident response. After incidents are resolved, you and your team conduct a root cause analysis. Doing this analysis helps you determine the underlying causes of declared incidents. Based on what you learn from the analysis, you can make changes to your network to prevent similar incidents.

Maintenance (MA) P1111: Perform maintenance on organizational systems.

REFERENCES

- NIST SP 800-171 3.7.1
- CERT RMM v1.2 TM:SG5.SP2

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

CLARIFICATION

Perform maintenance on your machines. This includes:

- corrective maintenance (e.g. repairing problems with the technology)
- preventative maintenance (e.g. updates to prevent potential problems)
- adaptive maintenance (e.g. changes to the operative environment)
- perfective maintenance (e.g. improve operations)

Example

You are in charge of IT at your company. As part of your role, you must perform maintenance on all the machines within your company. This includes regular planned maintenance, unscheduled maintenance, reconfigurations when required, and damage repairs. In addition to performing maintenance, you also keep track of all maintenance performed.

Maintenance (MA) P1112: Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

REFERENCES

- NIST SP 800-171 3.7.2

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

CLARIFICATION

Protect the tools used to perform maintenance. They must remain secure so they don’t introduce software viruses or other bugs into your system. Protect your maintenance processes so they aren’t used to hurt your network. Supervise the people responsible for maintenance activities. Make sure they don’t behave in a malicious manner.

Example

You are responsible for maintenance activities on your company’s machines. These activities can introduce software viruses or bugs into your system. To prevent this, make sure your maintenance tools protect from unauthorized access. Also, confirm that your organization manages or supervises everyone assigned to perform maintenance.

Maintenance (MA) P1113: Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

REFERENCES

- NIST SP 800-171 3.7.5

DISCUSSION [DRAFT NIST SP 800-171R2]

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

CLARIFICATION

Nonlocal maintenance activities must use multifactor authentication. Multifactor authentication requires at least two things to prove who the user says he is. One thing can be something you have, such as a device that generates a one-time passcode. Another thing can be something you know, for example, a password or passphrase. Or, another thing can be something specific to you, such as a fingerprint. Requiring two or more things to prove your identity increases the security of the connection. Nonlocal maintenance activities are activities conducted from external network connections. After nonlocal maintenance activities are complete, shut down the external network connection.

Example

You are in charge of conducting maintenance for your organization. Your employees are all remote. To maintain their devices, you establish a remote connection to their machines. When you log on to the remote connection, you must provide a one-time passcode and a token generated by a token device. You need both of these things to prove your identity. After you enter your password and passcode, you have access to the maintenance remote connection. When you finish your activities, shut down the remote connection.

Maintenance (MA) P1114: Supervise the maintenance activities of personnel without required access authorization.

REFERENCES

- NIST SP 800-171 3.7.6

DISCUSSION [DRAFT NIST SP 800-171R2]

This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

CLARIFICATION

You must supervise everyone who performs maintenance activities. Sometimes a person without proper permissions has to perform maintenance on your machines. Give that individual a logon that is active only once or for a very limited time, to limit system access.

Example

You are in charge of IT operations for your company. One of your software providers has to come on-site to update the software on your company’s machines. You give the individual a temporary logon and password that expires in 12 hours. This gives him access long enough to perform the update. When he is on site, you remain with him. You supervise his activities. This ensures that he performs only the maintenance activities you directed.

Media Protection (MP) P1119: Protect (i.e., physically control and securely store) system media containing Federal Contract Information, both paper and digital.

REFERENCES

- NIST SP 800-171 3.8.1
- CERT RMM V1.2 KIM:SG2.SP2

DISCUSSION [DRAFT NIST SP 800-171R2]

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

[SP 800-111] provides guidance on storage encryption technologies for end user devices.

CLARIFICATION

Physical Federal Contract Information (FCI) includes two types of items:

- hardcopy, for example, paper and microfilm
- digital devices, for example, CD drives, flash drives, and video

You should store physical FCI in a secure location. This location should be accessible only to those people with the proper permissions. All who access FCI should follow the process for checking out and returning it.

Example

Your organization has FCI for a specific Army contract. The Army gave you the FCI on a CD. You store the CD in a locked drawer and you log the FCI CD in an inventory. You also establish a procedure to check out the CD when your employees need to use it.

Media Protection (MP) P1120: Limit access to Federal Control Information on system media to authorized users.

REFERENCES

- NIST SP 800-171 3.8.2
- CERT RMM V1.2 MON:SG2.SP4

DISCUSSION [DRAFT NIST SP 800-171R2]

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

CLARIFICATION

Limit physical access to FCI to people permitted to access FCI. Use locked or controlled storage areas and limit access to only those allowed to access FCI. Keep track of who accesses physical FCI in some sort of record.

Example

Your organization has FCI for a specific Army contract. The Army gave you the FCI on a CD. You store the CD in a locked drawer. The only employees with access to the drawer are those assigned to the project. They are the only people allowed to access FCI. When someone removes the CD for work, they sign it out with their name and time. When they return the CD to the locked drawer, they sign it back in.

Media Protection (MP) P1121: Control the use of removable media on system components.

REFERENCES

- NIST SP 800-171 3.8.7
- CERT RMM V1.2 MON:SG2.SP4

DISCUSSION [DRAFT NIST SP 800-171R2]

In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices. 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

Removable media is any type of media storage that you can remove from your computer or machine, for example, CDs, DVDs, diskettes and USB drives. Write a specific policy for removable media for your company. Limit the use of removable media to the smallest number needed. Scan all removable

CLARIFICATION *(continued)*

media for viruses. Track removable media that you own and make sure you reuse and dispose of it properly.

Example

You are in charge of IT operations at your company. You establish a policy for USB drives. All of them must be scanned for viruses and bugs before use on the company's networks. You set up a separate computer to scan these drives before anyone uses them on the network. This computer has anti-virus software installed that is kept up to date.

Personnel Security (PS) P1127: Screen individuals prior to authorizing access to organizational systems containing Federal Contract Information.

REFERENCES

- NIST SP 800-171 3.9.1
- CERT RMM V1.2 HRM:SG2.SP1

DISCUSSION [DRAFT NIST SP 800-171R2]

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

CLARIFICATION

Make sure all employees who need access to FCI have the proper screening before they get access. Base the types of screening on the requirements defined for that specific level of access.

Example

You are in charge of security at your organization. All individuals you hire must have proper screening before they can access FCI. Screening may include activities such as background checks and drug testing. Follow the appropriate laws, policies, regulations, and criteria for the level of access required for each position.

Personnel Security (PS) P1128: Ensure that organizational systems containing Federal Contract Information are protected during and after personnel actions such as terminations and transfers.

REFERENCES

- NIST SP 800-171 3.9.2
- CERT RMM V1.2 HRM:SG2.SP2

DISCUSSION [DRAFT NIST SP 800-171R2]

Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

CLARIFICATION

Make sure employees no longer have access to FCI when they change jobs or leave the company. Confirm that when an employee leaves:

- they return all company IT equipment (e.g., laptops, cell phones, storage devices)
- they return all of their identification/access cards and/or keys
- conduct an exit interview to remind the employee of their obligations to not discuss FCI, even after employment

CLARIFICATION *(continued)*

The organization will do the following:

- erase all equipment before reuse
- remove access to all accounts granting access to FCI
- disable or close employee accounts
- limit access to physical spaces with FCI

Example

You are in charge of IT operations at your company. When someone leaves the company, you remove them from any physical FCI access lists. You contact them immediately, and ask them to:

- turn in their computers for proper handling which includes IT disabling all accounts
- return all their identification and access cards
- attend an exit interview where you remind them of their obligations to not discuss FCI

Physical Protection (PP) P1135: Protect and monitor the physical facility and support infrastructure for organizational systems.

REFERENCES

- NIST SP 800-171 3.10.2
- CERT RMM V1.2 KIM:SG4.SP2

DISCUSSION [DRAFT NIST SP 800-171R2]

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

CLARIFICATION

Make sure that the infrastructure inside of your facility, such as power and network cables, is protected so that visitors and employees cannot access it. The protection also has to be monitored. This can be done with security guards, video cameras, sensors and alarms.

Example

You are responsible for protecting your organization’s IT facilities. You install video monitoring at each entrance and exit. You also make sure there are secure locks on all entrances and exits to the facilities. This makes sure the IT facilities are safe from damage.

Recovery (RE) P1137: Regularly perform and test data back-ups.

REFERENCES

- ISO/IEC 27001 A.12.3.1
- NIST CSF v1.1 PR.IP-4
- CIS Controls v7.1 10.1 and 10.3

DISCUSSION

Back-ups are used to recover data in the event of a hardware or software failure. Back-ups should be performed regularly based on an organizational defined frequency. They should be tested regularly to ensure they are performing as expected.

CLARIFICATION

Back up your organizational data so you can recover it if a hardware failure, software failure, or malware infection occurs. You can schedule backups to run automatically or manually. Many operating systems include a built-in feature to perform data backups.

After you create a backup, it is important to test it on a regular basis. When you test a backup, verify that the operating system, applications, and data are intact and functional. If you test data backups regularly, you will be in a better position to recover systems and files more efficiently if a failure or infection occurs.

Example

You are responsible for IT in your organization. One of your jobs is to make sure you can restore data if a serious event happens, such as a disaster, a hard drive failure, or a software problem. You have a back-up procedure in place where you back up all your data weekly on a back-up server. You set this up to occur automatically each weekend because it takes a lot of resources to perform a back-up. You verify your back-ups every month. This ensures that your data is correct. It also confirms that you can use the data if you need to recover your systems.

Recovery (RE) P1138: Protect the confidentiality of backup Federal Contract Information at storage locations.

REFERENCES

- NIST SP 800-171 3.8.9
- CERT RMM v1.2 MON:SG2.SP4

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

CLARIFICATION

You protect the confidentiality of information to ensure that it remains private and unchanged. Methods to ensure confidentiality may include:

- encrypting files
- managing who has access to the information
- physically securing devices and media that contains FCI
- managing the use of information

Storage locations for information are varied, and may include:

- external hard drives
- USB flash drives
- disc media (CD/DVD/Blu-Ray)
- Networked Attached Storage (NAS)
- cloud backup
- FTP/FTP Secure/SFTP

Example

You are in charge of protecting Federal Contract Information for the company. You need to protect the confidentiality of backup data. You encrypt all your FCI data as it is saved on an external hard drive. Only people who are on the contract can access the hard drive. You secure the external hard drive in a physical location accessible only to people with permission.

Risk Management (RM) 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.

REFERENCES

- NIST SP 800-171 3.11.1
- CERT RMM v1.2 RISK:SG4

DISCUSSION [DRAFT NIST SP 800-171R2]

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

[SP 800-30] provides guidance on conducting risk assessments.

CLARIFICATION

Organizations should assess the risk to their operations and assets at regular intervals. Risks to consider may include:

- poorly designed and executed business processes
- inadvertent actions of people, such as disclosure or modification of information
- intentional actions of people, such as insider threat and fraud
- failure of systems to perform as intended
- failures of technology
- external events, such as natural disasters, public infrastructure and supply chain failures

An organization can perform a formal or an informal risk assessment. In a formal risk assessment, you use established criteria and procedures. Formal risk assessments are documented.

Example

You help manage IT for your employer. You and your team members are working on a big government contract where you have to store FCI. You assess the risk involved with storing FCI. You consider storing that information with a cloud provider. You and your coworkers discuss the pros and cons of this option. Then, you use these details to make the final decision about using a cloud provider.

Risk Management (RM) P1142: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

REFERENCES

- NIST SP 800-171 3.11.2

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

[SP 800-40] provides guidance on vulnerability management.

CLARIFICATION

A vulnerability scanner is an application that identifies an organization’s asset vulnerabilities for which the scanner is capable of identifying. Then, the scanner creates a prioritized list of asset vulnerabilities

CLARIFICATION *(continued)*

ordered by their level of severity. The scanner also describes each vulnerability and the steps needed to fix it. Your organization should scan for vulnerabilities on all devices connected to the network. This includes servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers. All assets that have any form of connection to a wired network, Wi-Fi environment, and air-gapped labs that are associated with the CMMC assessment.

Organizations that develop custom software should perform reviews of the software. Vulnerability analysis of a custom-made solution requires an experienced penetration tester to properly test and validate findings. Automated vulnerability scanners do not necessarily perform well against custom developed applications.

The vulnerability scanning process should, should be a regular activity. It should not be a single occurrence. Organizations should put in place a vulnerability scanner that updates its database each time it performs a scan. This means that the scan looks for the most current vulnerabilities. Schedule sans so that they do not have an impact on normal operations. Use caution when scanning critical assets. These assets do need to be scanned, but some scanning options could cause a denial of service against a critical asset. You could replicate the critical asset in a test environment and perform vulnerability scans against the replicated asset. The replicated asset vulnerability scan will produce valid reports that need to be applied to the production system only if the replicated system is an exact duplicate of the production system and has identical functionality in operation when being tested.

Example

You are in charge of IT in your organization. You look for errors in your software that may provide ways for hackers to get into your network and do harm. You perform vulnerability scans to try and find these errors. You use a vulnerability scanner application that tests all the assets connected to your network. As a result of the scan, you get a prioritized list of vulnerabilities. Because you will scan everything connected to your network, you should set up the scan to happen at night. You should also make sure that your vulnerability scanner application gets updated on a regular basis.

Risk Management (RM) P1143: Remediate vulnerabilities in accordance with risk assessments.

REFERENCES

- NIST SP 800-171 3.11.3
- CERT RMM v1.2 VAR:SG3.SP1

DISCUSSION [DRAFT NIST SP 800-171R2]

Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

CLARIFICATION

Review the prioritized list of vulnerabilities generated from the vulnerability scanner. Not all vulnerabilities may affect an organization the same. Review the risks of not remediating the discovered vulnerabilities. The organization should build upon the prioritized list a develop a prioritized mitigation plan for closing the vulnerabilities identified and track their completion.

Example

You are in charge of IT at your organization. Part of your job is to look for weaknesses in your software that may provide ways for hackers to get into your network and do harm. You perform vulnerability scans to try and find these weaknesses. The output of a scan is a list of the potential weaknesses, also called vulnerabilities. You should review the vulnerabilities and determine how they will affect your organization. You should create a prioritized list of the vulnerabilities you should fix, fix them, and record a completion date and time by each item. If you decide not to fix them, you should document the reasoning, and you should continue to monitor these vulnerabilities.

Security Assessment (SAS) 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.

REFERENCES

- NIST SP 800-171 3.12.4

DISCUSSION [DRAFT NIST SP 800-171R2]

System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

[SP 800-18] provides guidance on developing security plans.

CLARIFICATION

A system security plan (SSP) is a document that outlines how an organization implements its security requirements. An SSP outlines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows. An SSP should include high-level diagrams that show how connected systems talk to each other. The organization should outline in its SSP its design philosophies. Design philosophies include defense-in-depth strategies as well as allowed interfaces and network protocols. All information in the SSP should be high-level. Include enough information in the plan to guide the design implementation of the organization’s systems. Reference existing policies and procedures in the SSP. An SSP should include all unmet requirements, as well as the plan to meet them.

Example

You are in charge of system security in your organization. As part of your job, you develop a system

Example *(continued)*

security plan (SSP). The SSP tells all employees how they can meet the organization's system security goals. The information in the SSP should explain how you should handle your important information. Examples include who can access important information, where you should store it, and how you can transmit it. By defining a clear SSP, you can design and build your network to ensure that it meets the SSP-defined goals. You can also use your SSP to outline the organization's:

- security requirements
- the current status of the requirements
- your plan to meet the requirements in the future

Security Assessment (SAS) P1158: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

REFERENCES

- NIST SP 800-171 3.12.1

DISCUSSION [DRAFT NIST SP 800-171R2]

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

[SP 800-53] provides guidance on security and privacy controls for systems and organizations. [SP 800-53A] provides guidance on developing security assessment plans and conducting assessments.

CLARIFICATION

As organizations implement security controls, they should avoid a “set it and forget it” mentality. The security landscape is constantly changing. Reassess existing controls at periodic intervals in order to validate their usefulness in organizational systems. This will let you determine if the control is still meeting the needs of the organization. Set the assessment schedule according to organizational needs. Consider regulatory obligations and internal policies when assessing the controls.

CLARIFICATION *(continued)*

Typical outputs of the practice include:

- documented assessment results
- proposed new controls, or updates to existing controls
- remediation plans
- new identified risks

Example

You are in charge of IT operations in your company. You ensure that security controls are achieving their objectives. After you implement the controls, you monitor their performance. You should perform this review at a as often as necessary to meet:

- your organization’s risk planning needs
- any regulations or policies you must follow

When you assess the controls, document what you find. When you find your controls are not meeting your requirements, you should act and make changes. You can:

- propose updated or new controls
- develop a plan to improve the control
- document new risks that you find

You should also document these actions.

Security Assessment (SAS) P1159: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

REFERENCES

- NIST SP 800-171 3.12.2

DISCUSSION [DRAFT NIST SP 800-171R2]

The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

CLARIFICATION

When you write a plan of action, you should define the clear goal or objective of the plan. You may include the following in the action plan:

- ownership of who is accountable for ensuring the plan’s performance
- specific steps or milestones that are clear and actionable
- responsibility for each step
- milestones to measure plan progress
- completion dates

Example

You are in charge of IT operations in your organization. Your job is to develop action plans when you discover that your company isn’t meeting security requirements. One of your sources of information is the output of vulnerability scans on your network. When you receive notification of a vulnerability that needs fixing, you develop a plan to fix it. Your plan identifies the person responsible for fixing it, how to do it, and when to do it. You will also define how to measure that the person responsible has fixed the vulnerability. You document this in a plan of action.

System and Communications Protection (SCP) P1178: Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

REFERENCES

- NIST SP 800-171 3.13.12

DISCUSSION [DRAFT NIST SP 800-171R2]

Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

CLARIFICATION

You should configure collaborative computing devices so they cannot be activated remotely. Examples of such devices are cameras, microphones, etc. All users should receive a notification when a collaborative computing device is in use. Notification can include an indicator light that turns on when in use, or a specific text window that appears on screen. If a device does not have the means to alert a user when in use, the organization should provide manual means. Manual means can include, as necessary:

- paper notification on entryways
- locking entryways when a collaborative computing device is in use

Example

You are responsible for IT operations in your organization. Your organization has a group of remote employees who collaborate using cameras and microphones attached to their computers. You want to prevent the misuse of these devices. You disable the ability to turn on cameras or microphones remotely on all devices. You also use a tool to alert users when their cameras or microphones are turned on. This enables them to see if the devices were activated remotely. By doing this, you reduce the likelihood of someone being able to turn these devices on and listen or view what your employees are working on.

System and Communications (SCP) P1179: Use encrypted sessions for the management of network devices.

REFERENCES

- CIS Controls v7.1 11.5

DISCUSSION [DRAFT NIST SP 800-171R2]

Authenticity protection includes, for example, protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

NIST Special Publications 800-52, 800-77, 800-95, and 800-113 provide guidance on secure communications sessions.

CLARIFICATION

When an organization connects to and manages network devices, it should use an encrypted session. The most common encrypted method is a Secure Shell (SSH).

Example

You are an IT administrator for your organization. You are in charge of updating devices on your network. You access these devices over the network instead of at the device's physical location. When you establish a connection to these devices, you use an SSH connection. An SSH connection protects you. For example, an adversary has installed malware on a network device. If you use an unencrypted session (i.e., telnet into a device) the adversary can view your username and password. But, if you use an SSH connection, the adversary cannot see this information.

System and Informational Integrity (SII) P1214: Monitor system security alerts and advisories and act in response.

REFERENCES

- NIST SP 800-171 3.14.3
- NIST CSF v1.1 RS.AN-5

DISCUSSION [DRAFT NIST SP 800-171R2]

There are many publicly available sources of system security alerts and advisories. The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations

[SP 800-161] provides guidance on supply chain risk management.

CLARIFICATION

Organization should receive security alerts, advisories, and directives from reputable external organizations. You base identification of these organizations on sector, industry, and the technology you use . There are many ways to received alerts and advisories and may include:

- signing up for email distributions
- subscribing to RSS feeds
- attending meetings

Organizations should review alerts and advisories for applicability as they receive them. An organization decides on its own review cycle. The more frequent the alerts and advisories, the more frequent the reviews. This ensures that the organization has the most up-to-date information.

External alerts and advisories may prompt an organization to generate internal security alerts, advisories, or directives. Shared these with all personnel with a need-to-know. The individuals should act to respond to the alerts. Actions vary according to the alert or advisory. Sometimes it may require a system configuration update. Other times, the organization may use the information for situational awareness purposes.

Example

You are in charge of IT operations in your company. You should pay attention to organizations that provide you with security alerts and advisories. You decide to receive alerts from US-CERT and a set of

Example *(continued)*

ISACs. You review the alerts on a weekly basis, then decide if they are of interest to your organization. If you find an alert to be of interest, you should develop an approach for acting on the alert. For example, you hear about a known bug in software that you use. You should develop and implement a plan for patching that software as soon as possible.

System and Informational Integrity (SII) P1216: Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

REFERENCES

- NIST SP 800-171 3.14.6

DISCUSSION [DRAFT NIST SP 800-171R2]

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[SP 800-94] provides guidance on intrusion detection and prevention systems.

CLARIFICATION

Organizations should leverage their monitoring systems to look for indicators of attacks. Think of indicators of attack as a series of actions that an adversary conducts in advance of an attack. Indicators of attack concern the steps involved and the intent of the adversary.

CLARIFICATION *(continued)*

Indicators of attacks on organizational systems may include:

- internal traffic that indicates the presence of malicious code
- malicious code detected during non-business hours
- the unauthorized data leaving the organization
- communicating to external information systems

To detect attacks and indicators of attacks with success, deploy monitoring devices. Place these devices within the systems at strategic points to collect essential information. Strategic points include internal and external system boundaries. The organization should monitor both inbound traffic and outbound traffic.

Example

You are in charge of IT operations at your organization. You look for attacks to your network. To do this, you monitor all organizational systems. You also watch communications to and from your machines. You look for indicators, or things that don't look like they should. These indicators can show up in many places on your network. You should monitor important places on your network. These places might include:

- perimeter locations, or locations your networks connect to the internet
- machines that have important software or data on them that attackers might want to access
- your remote connections which may be a way to gain access to your network from the outside

Perform additional monitoring when you find an indicator, or something that doesn't perform as it should. This extra monitoring should tell you if it is a current or potential attack.

Set up your monitoring activities so that they support your organization's planning. Develop your monitoring requirements as part of your organization's security activities. Ensure that your monitoring activities meet the security needs of your organization.

System and Informational Integrity (SII) P1217: Identify unauthorized use of organizational systems.

REFERENCES

- NIST SP 800-171 3.14.7

DISCUSSION [DRAFT NIST SP 800-171R2]

System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[SP 800-94] provides guidance on intrusion detection and prevention systems.

CLARIFICATION

Organizations should define authorized use of their systems. First, have an acceptable-use policy for your system. This policy establishes the baseline for how users access devices and the internet. You define authorized use by specific roles within the organization. Examples of these roles include user, administrator, and technician. After you define authorized use, identify unauthorized use of systems.

Organizations can monitor systems by observing audit activities. You can do this in real time or by other manual means, such as access patterns. To identify unauthorized use, leverage existing tools and techniques, such as:

- intrusion detection systems
- intrusion prevention systems
- malicious code protection software
- scanning tools
- audit record monitoring software
- network monitoring software

Example

You are in charge of IT operations at your organization. You want to make sure everyone using an organizational system is authorized to do so. You accomplish this as part of your monitoring activities. These activities ensure that all users meet the defined authorize-use policy. To do this, you put in place a user activity monitoring application. This app monitors all the users and their connections to your network. It records information about every connection on your network. You use the outputs of this application to confirm that you are meeting the authorization policy.

APPENDIX D. CMMC LEVEL 3 DISCUSSION AND CLARIFICATION (EXCLUDING NIST SP 800-171 PRACTICES)

Introduction

This draft provides discussion and clarifications for the CMMC Level 3 practices which are not already described by NIST 800-171 Revision 1.

Please note that the clarification examples are intended only to help explain the practices and do not represent guidance.

Asset Management (AM) P1035: Identify, categorize, and label all CUI data.

REFERENCES

- ISO/IEC 27001 A.8.2.1
- ISO/IEC 27001 A.8.2.2

DISCUSSION

The intent of identifying, categorizing and labeling CUI is to ensure that the information receives the protection required based on organizational, legal and contractional requirements.

In order to ensure that the necessary protections for CUI are in place, the data should be categorized based on sensitivity and labeled so that it is handled properly.

Note: This practice deals with identifying, categorizing and labeling of CUI. The organization should also define procedures for the handling of CUI according to practice AM.P1036 .

CLARIFICATION

Establish procedures for identifying, categorizing, and labeling all information determined to meet the criteria of CUI. The procedures should account for both physical and digital CUI.

Example

As a manager for a government program that contains CUI, you ensure that there are defined procedures for identifying, categorizing, and labeling CUI. This includes how you will identify CUI that you receive either electronically or in hard copy. You also establish a procedure for categorizing and tracking your CUI, so that you can ensure that only the people with proper permissions have access to the CUI. In addition, you ensure that both your electronic and physical CUI is labeled appropriately in accordance with your standard operating procedures.

Asset Management (AM) P1036: Define procedures for the handling of CUI data.

REFERENCES

- ISO/IEC 27001 A.8.2.3

DISCUSSION

The organization should define procedures for the proper handling of CUI. These procedures typically involve establishing controls to protect and sustain sensitive information. Examples of controls an organization may implement through data handling procedures include policies (data categorization, disposal, backup), access controls for data, regular backups and physical security protections.

Note: This practice deals with defining procedures for the handling of CUI. The identification, categorization, and labeling of CUI is covered in AM:P1035

CLARIFICATION

Establish procedures for handling CUI. Procedures should include how to receive, transmit, store, and destroy CUI information. The procedures should account for both physical and digital CUI.

Example

As a manager for a government program that contains CUI, you ensure that you have defined procedures for handling CUI. This includes how you will receive both electronic and physical CUI from the government. Additionally, you define the requirements for how you will transmit CUI, either electronically or physically. This may include requiring encryption for digital data, or requiring chain of custody logs for physical data, such as hard drives, discs, or printed material containing CUI.
Also, you specify how you should store CUI:

- in what form (i.e., encrypted for digital data or in a locked cabinet for physical data)
- in what location
- under what specific retention policies

You define a procedure for destroying CUI when it is no longer in use or required by the contract.

Audit and Accountability P1048: Collect audit logs into a central repository.

REFERENCES

- CMMC

DISCUSSION

Aggregate and store audit logs in a central location. The central repository enables analysis by storing audit record content needed for analysis in a common location and format. Storing audit logs in a central repository also protects audit information. The repository has the available infrastructure, capacity, and protection mechanisms to meet the organization's audit requirements.

CLARIFICATION

Aggregate and store audit logs in a centralized location within the organization. Storing audit logs in a centralized location place supports analysis activities by enabling a full picture of the audit logs, and can support automated analysis capabilities. Ensure that the central repository has the appropriate infrastructure, including protection mechanisms, and the capacity level to meet the logging requirements of the organization. Additionally, define logging data retention and storage policies.

Example

You are in charge of IT operations in your organization. Your responsibilities include reviewing audit logs. You consolidate all audit logs in a common format and into a centralized logging infrastructure that may consist of one or more servers. By doing this, you enable centralized analysis of your audit logs. This increases situational awareness across your network. In addition, you are able to better protect your audit logs by storing them in one centralized location.

Recovery (RE) P1139: Regularly perform complete and comprehensive data back-ups as organizationally defined and store them off-site and offline.

REFERENCES

- CIS Controls v7.1 10.1, 10.2, and 10.5

DISCUSSION [CIS CONTROLS V7.1 10]

Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of data.

Why Is This CIS Control Critical?

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with information that has been modified with malicious intent. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker’s presence on the machine.

10.1 Ensure that all system data is automatically backed up on a regular basis.

10.2 Ensure that all of the organization’s key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

10.5 Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

CLARIFICATION

Ensure all systems and data are backed up at an interval that enables an organization to restore the system or data in accordance with their business requirements. You should complete the backups frequently, and on a regular schedule that satisfies the needs of your organization. You should consider storing at least one system backup off-site and offline to provide redundancy in the event of a disaster. The interval and complexity of your data recovery capabilities can be informed by reviewing your service level agreement with your DoD customer.

Example

You are in charge of IT operations for your organization. As part of your responsibilities, you create backups of all your system data. You do this to meet the business objectives of your organization as outlined in your service level agreements with your customers. Meeting these objectives will help you manage the loss of data availability or corrupted data in the event of a cyber incident. For example,

Example *(continued)*

you may conduct full system backups every Friday evening after business hours. You store your backups offline at a different location than your other systems. Doing this provides added protection of your backups from a cyber event or physical disaster that may impact your organization.

Risk Management (RM) P1144: Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

REFERENCES

- NIST CSF ID.RA
- CERT RMM v1.2 RISK:SG3 and SG4.SP3

DISCUSSION [NIST CSF]

NIST CSF ID.RA: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

CLARIFICATION

Risk assessments are performed to identify potential risks to the organization. A risk assessment identifies risks to organization functions and the supporting assets: people, technology, information, and facilities. Threat information, vulnerabilities, likelihoods, and impacts are used to identify risk. Evaluate and prioritize the identified risks based on the defined risk criteria: risk sources, risk categories, and risk measurement criteria.

It is important to note that risk assessments differ from vulnerability assessments. A vulnerability assessment focuses primarily on technical vulnerabilities in a system, and provides input to a risk assessment. A risk assessment may not be a strictly technical assessment. Also, it includes such qualitative data as likelihood analysis and potential threat descriptions. Refer to RM:P1142 for vulnerability assessments.

Example

You are in charge of risk management for your organization. As part of your duties, you perform risk assessments quarterly, or when you have a significant change to your environment. Such a change includes notification of a new threat, of the acquisition of a new system or environment, or of a new contract requirement. To perform your risk assessment, you identify your organizational functions and the assets required to support them. You use all available sources, such as threat information, vulnerability scan results, and previous risk assessments. This enables you to identify potential risks to your organization. You have a risk management policy in place that defines your risk criteria, including risk sources, risk categories, and risk measurement criteria. You use this risk criteria to prioritize your risks based on what is likely to harm your organization the most. You use the output to prioritize the actions you take to address your organization's risks.

Risk Management (RM) P1146: Develop and implement risk mitigation plans.

REFERENCES

- NIST CSF ID.RA-6
- CERT RMM v1.2 RISK:SG5.SP1

DISCUSSION [CERT RMM V1.2]

ID.RA-6: Risk responses are identified and prioritized

RISK:SG5:SP1 Develop Risk Response Plans

Risk response plans are developed.

When the consequences of risk exceed the organization's risk thresholds and are determined to be unacceptable, the organization must act to address risk to the extent possible.

Addressing risk requires the development of response strategies that may include a wide range of activities. In some cases, risk response will require adjustments to current strategies for protecting and sustaining assets and services. In other cases, the organization will find itself designing and

implementing new controls and service continuity plans. In addition, because not all risk can be mitigated, the organization must be able to address residual risk—the risk that remains and is accepted by the organization after response plans are implemented.

This risk must be analyzed and determined to be acceptable before the risk response plan is in place.

CLARIFICATION

For each identified risk, develop and implement a risk mitigation plan. Mitigation plans should define a risk disposition for each identified risk. Possible risk dispositions include: avoid, accept, monitor, defer, transfer, and mitigate. Mitigation plans define how to address or limit the identified risk. Risk mitigation plans may include:

- how the vulnerability or threat will be reduced
- the actions that will limit risk exposure
- controls to be implemented
- staff responsible for the mitigation plan
- the resources required for the plan
- the implementation specifics (when, where, how)
- how the plan implementation will be measured or tracked

Example

You are in charge of risk management for your organization. You develop risk mitigation plans for your organization's identified risks. You create a template to develop your risk mitigation plans. Your

Example *(continued)*

template includes:

- the actions or potential controls you will implement
- who will perform the actions
- when, where, and how the actions will take place
- how you will track the plan to completion

Risk Management (RM) P1147: Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.

REFERENCES

- CMMC

DISCUSSION

Unsupported products are products that are no longer supported by the developer. When a product becomes unsupported, there are no security updates and patches, putting the system at an increased risk. Manage unsupported products separately than your supported products to reduce exposure.

CLARIFICATION

When a vendor no longer supports your organization's products, you do not receive critical software updates and security updates. This puts your organization at risk because vulnerabilities may remain unpatched. In addition, the product may not work properly with newer systems on your network. This can create technical problems within your network as well.

To mitigate these risks, you should manage unsupported products separately. The management of these products may include the following.

- Define risk exposure caused by unsupported products. Ensure that you monitor the risk within your organization's defined risk criteria.
- Remove and isolate unsupported products from your organization's network.
- Upgrade, retire, or replace unsupported products.

Example

You are in charge of IT operations at your organization. Unfortunately, you don't have the budget to update one of your systems, which the vendor no longer supports. Because you know this creates an increased risk, you manage this system separately from your supported systems. First, you make sure you understand the potential risks that this unsupported machine introduces into your network. Then, you take appropriate actions to mitigate these additional risks.

- You make sure any residual risk is within your organization's risk threshold, and continue to monitor the risk.
- You ensure that this system is isolated from your organization's operational network and the internet so that it does not introduce additional vulnerabilities into your network.
- You develop a plan for upgrading or replacing the machine when funding becomes available.

Security Assessment (SAS) P1162: Employ code reviews of enterprise software that has been developed internally for internal-use to identify areas of concern that require additional improvements.

REFERENCES

- CMMC

DISCUSSION

Software applications that are developed in-house for internal use are reviewed for security checks to ensure there are no accidental errors that may introduce vulnerabilities into an organization's network. The code review can be manual or automated.

CLARIFICATION

All in-house developed software should be reviewed by an organizational representative trained and responsible for the evaluation of internally developed software using static and/or dynamic application security testing tools.. The purpose of the code review is to provide the organization and its customers and partners assurances that the code has undergone sufficient testing. This testing is used to identify and mitigate errors within the codebase that may introduce unintentional process flow that could lead to an exploitable vulnerability.

Example

You are in charge of IT operations for your organization. You have a group of developers who create internal software applications. Because you develop the software in house, you make sure the code is reviewed so that code mistakes do not result in vulnerabilities. You have another software engineer, who is not part of the development team, perform a manual code review to ensure the software is safe. You do this for each software update or iteration. You prohibit the software from being run on the organization's network until the code review is complete.

Situational Awareness (SA) P1169: Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.

REFERENCES

- CMMC

DISCUSSION

Establish relationships with external organizations to gather cyber threat intelligence information. Cyber threat information from external sources should inform situational awareness activities within the organization. Relevant external threat information is communicated to stakeholders within the organization for appropriate action if needed.

CLARIFICATION

To enhance situational awareness activities within the organization, leverage external sources for cybersecurity threat information. Establish a relationship with external organizations, or periodically survey relevant sources, to ensure you are receiving up-to-date threat intelligence information pertinent to your organization. Examples of sources include: US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, and federal briefings.

Threat information is reviewed and, if applicable to your organization, communicated to the appropriate stakeholders for action.

Example

You are in charge of IT operations for your company. Part of your role is to ensure you are aware of up-to-date cyber threat intelligence information so you can properly perform risk assessments and vulnerability analyses. To do this, you join a defense sector ISAC, and sign-up for alerts from US-CERT. You use information you receive from these external entities to update your threat profiles, vulnerability scans, and risk assessments. Also, you use these sources to gather best practices for informing your employees of potential threats and disseminate the information throughout your organization to the appropriate stakeholders.

System and Communications Protection (SCP) P1192: Implement Domain Name System (DNS) filtering services.

REFERENCES

- CMMC
- CIS Controls v7.1 7.7

DISCUSSION [CIS CONTROLS V7.1 7]

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Why Is This CIS Control Critical?

Web browsers and email clients are very common points of entry because of their technical complexity, flexibility, and direct interaction with users, systems, and websites. Content can be crafted to entice users to take actions that greatly increase risk of organizational compromise and allow the introduction of malicious code and loss of valuable information such as CUI . Historically speaking, threat actors routinely enter an organization's network through phishing emails and the introduction of malicious content onto trusted websites, thus making the protection of these entry points critical to an organization's defensive strategy.

7.7: Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

CLARIFICATION

Domain Name System (DNS) filtering blocks access to certain websites or IP addresses. The organization should use DNS to block known malicious websites or categories of websites. A commercial DNS filtering service can be used.

Example

You are in charge of IT operations for your company. Part of your role is to implement web browser protections. To do this, you purchase a commercial DNS filtering application or service and configure your enterprise environment to use the service. The configuration blocks users from being able to access known malicious websites. The application provider is responsible for ensuring it has the latest list of known malicious websites. As an administrator, you can update this filtering mechanism for your organization, as appropriate, to provide additional DNS blocking or to allow previously blocked websites. Although the DNS provider is responsible for maintaining an up-to-date list of known malicious websites, you are still accountable to your organization's leadership and must therefore monitor the service for effectiveness.

System and Communications (SCP) P1193: Implement a policy restricting the publication of CUI on publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter, etc.).

REFERENCES

- CMMC

DISCUSSION

Define and enforce a policy that restricts employees from publishing CUI on public websites such as forums and social media outlets.

CLARIFICATION

Establish a defined and communicated policy to prohibit employees from posting CUI on a publicly facing website. This includes social media outlets such as Facebook, LinkedIn, and Twitter.

Example

You are a program manager for a contract that uses CUI. To ensure you are protecting your information correctly, you inform everyone working on the project of your existing policy that prohibits the posting of CUI on public websites. This includes any job- or industry-related forums or discussions that may reference your contract work.

System and Informational Integrity (SII) P1218: Employ spam protection mechanisms at information system access entry and exit points.

REFERENCES

- CMMC

DISCUSSION

Spam filtering is used to protect against unwanted, unsolicited, and often harmful emails from reaching end user mailboxes. Spam filters are applied on inbound and outbound emails. Spam filtering helps protect your network from phishing and emails containing viruses and other malicious content. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers.

CLARIFICATION

Spam filters should be applied on email that is inbound (coming into the organization) or outbound (leaving the organization). Inbound filters can protect the organization’s users from spam originating on the internet. Outbound protection helps the organization identify the origins of potential spam on their own network. Without this, an organization risks having its email server blacklisted for sending spam emails.

Example

As the email administrator for your company, you notice a significant increase in the amount of spam entering your network year after year. You want to implement a spam filtering capability to meet these two goals:

- reduce the number of unsolicited email to your user’s inboxes
- block potentially harmful email, including phishing emails and attachments, from reaching end users

You are also concerned that, without adding outbound spam protections, your organization’s email servers could be blacklisted. Because of this, you implement outbound protections that allow you to trace potential spam email originating on your network to a specific user and machine.

System and Informational Integrity (SII) P1219: Implement email protections such as DNS or asymmetric cryptography.

REFERENCES

- CMMC

DISCUSSION

Protecting your environment from harmful emails is one of the best ways to reduce the risk of viruses and malware from entering your network. Email attacks are one of the primary attack vectors in use by threat actors today because of their simplicity and effectiveness for circumventing an organization’s perimeter defenses. Implementing advanced email protections can help mitigate these email-based threats from penetrating an organization’s defenses and landing in the inbox of organizational end users.

CLARIFICATION

Implement more email protections in addition to basic spam protections. Some potential more advanced email protections include Sender Policy Framework (SPF) ,Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC). SPF uses DNS to show which servers are allowed to send email for a given domain. DKIM uses asymmetric cryptography to verify the authenticity of an email message, and DMARC allows organizations to deploy a combination of DKIM and SPF to further enhance their electronic mail infrastructure.

Example

As the email administrator for your organization, you want to add additional protections to ensure you are blocking as many unwanted and harmful emails as possible. You configure a DMARC policy that enables both SPF and DKIM on your domain. You configure an SPF text entry in your DNS configuration so that you explicitly authorize the servers that can send email as well as ensuring relevant outbound emails are signed using DKIM.

System and Informational Integrity (SII) P1220: Utilize email sandboxing to detect or block potentially malicious email attachments.

REFERENCES

- CIS Controls v7.1 7.10

DISCUSSION [CIS CONTROLS V7.1.7]

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Why Is This CIS Control Critical?

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

7.10: Use sandboxing to analyze and block inbound email attachments with malicious behavior.

CLARIFICATION

You create an email sandbox by implementing an isolated test environment to execute an attached file or linked URL. Before allowing attachments or links to be opened on the production network, they are tested within the sandbox and their behavior is observed. By opening these files or links in a protected environment, the system detects malicious activity before it is introduced into the network.

Example

You are in charge of IT operations for your organization. Part of your role is to verify all attachments and URL links in company emails. To do this, you set-up an isolated environment, or email sandbox, to execute or open all email attachments before allowing them on your network. You use the email sandbox to observe what happens when the attachment or link opens. By testing these files in a sandbox, you are able to prevent the entry of malicious content through email attachments or URL links.

APPENDIX E. CMMC MATURITY PROCESS DISCUSSION AND CLARIFICATION

Introduction

This draft provides discussion and clarifications for the CMMC maturity processes.

Please note that the clarification examples are intended only to help explain the practices and do not represent guidance.

Maturity Level (ML) MP001: Establish a policy that includes [DOMAIN NAME].

REFERENCES

- CERT RMM V1.2 GG2.GP1 Subpractice 2

DISCUSSION [CERT RMM V1.2 GG2.GP1 SUBPRACTICE 2]

Develop and publish organizational policy for the process.

Establish the organizational expectations for planning and performing the process, and communicate these expectations via policy. The policy should reflect higher level managers' objectives for the process.

CLARIFICATION

A policy is a high-level statement from an organization's senior management that documents the requirements for a given activity. It is intended to establish organizational expectations for planning and performing the activity, and communicate those expectations to the organization. Senior management should sign policies to show its support of the activity.

At a minimum, the policy should:

- clearly state the purpose of the policy
- clearly define the scope of the policy: for example, enterprise-wide, department-wide, or information-system specific
- describe the roles and responsibilities of the activities covered by this policy: the responsibility, authority, and ownership of [DOMAIN NAME] domain activities
- establish or direct the establishment of procedures to carry out and meet the intent of the policy, include any regulatory guidelines this policy addresses

Maturity Level (ML) MP002: Establish practices to implement the [DOMAIN NAME] policy.

REFERENCES

- CERT RMM V1.2 GG

DISCUSSION [CERT RMM V1.2 GG]

Practices are established, documented, and followed to implement the policy for [DOMAIN NAME].

CLARIFICATION

Practices discuss the specific activities involved in satisfying the intent of the related policy. The practices define the activity and prescribe the specific activities involved to meet the policy.

Documented practices inform that individuals responsible for a task or activity are able to perform it in a repeatable way. Organizations build the capability by documenting the process, then practicing it as documented, in other words “Say what you do; do what you say.”

The level of detail of a documented practice can vary, from a handwritten desk procedure to a formal organizational standard operating procedure that is managed and controlled.

The practices must include all activities in the [DOMAIN NAME] domain, up to the level of CMMC assessment. For example, CMMC Level 2 certification requires all Level 1 and Level 2 activities to be included in the practice documentation. CMMC Level 3 assessment requires all Level 1, Level 2, and Level 3 activities to be included.

Maturity Level (ML) MP003: Establish a plan that includes [DOMAIN NAME].

REFERENCES

- CERT RMM V1.2 GG2.GP2

DISCUSSION [CERT RMM V1.2 GG2.GP2]

Establish and maintain the plan for performing the process. In this practice, the organization determines what is needed to perform the process and to achieve the established objectives, to prepare a plan for performing the process, to prepare a process description, and to get agreement on the plan from relevant stakeholders.

CLARIFICATION

The organization establishes a plan for achieving the [DOMAIN NAME] activities.

The plan for performing the [DOMAIN NAME] activities typically includes:

- a mission statement and/or vision statement
- strategic goals/objectives, preferably in SMART format (**S**pecific, **M**easurable, **A**ttainable, **R**esult-focused, **T**ime-bound)
- relevant standards and procedures
- a project plan to record activities, due dates, and organizational resources (funding, people, tools, etc.) assigned to the management or oversight of [DOMAIN NAME] activities
- training needed to perform the [DOMAIN NAME] activities
- involvement of relevant stakeholders

Maturity Level (ML) MP004: Review [DOMAIN NAME] activities for adherence to policy and practices.

REFERENCES

- CERT RMM V1.2 GG2.GP9

DISCUSSION [CERT RMM V1.2 GG2.GP9]

Objectively evaluate adherence of the process against its process description, standards, and procedures, and address noncompliance.

The purpose of this process is to provide assurance that the process is implemented as planned and adheres to its process description, standards, and procedures as evidenced through an evaluation of selected work products of the process. The evaluation must be independent; that is, those directly involved in the performance of the process cannot perform the objective evaluation or render an opinion on adherence.

CLARIFICATION

[DOMAIN NAME] activities should be evaluated for adherence to policy and procedures. The purpose of this is to ensure the activities are producing the expected outcomes by ensuring policy and procedures are being appropriately followed.

For adherence to the [DOMAIN NAME] plan, the organization defines and conducts periodic reviews needed to ensure that:

- practices are performed as planned and adhere to process descriptions, standards, and procedures
- deviations from stated practices are identified and evaluated
- problems in the practices for performing [DOMAIN NAME] activities are identified
- non-compliance is addressed
- needed process changes are identified when expected results or outputs are not met

Maturity Level (ML) MP005: Provide adequate resources for meeting the plan for [DOMAIN NAME] activities.

REFERENCES

- CERT RMM V1.2 GG2.GP3

DISCUSSION [CERT RMM V1.2 GG2.GP3]

Provide adequate resources for performing the process, developing the work products, and providing the services of the process.

This process focuses on providing the resources necessary to perform the process as defined by the plan and ensuring that resources are available when needed. Resources are formally identified and assigned to process plan elements.

Resources include an adequate number of *skilled* staff, expense and capital funding, facilities, tools, techniques, and methods.

CLARIFICATION

Resources for [DOMAIN NAME] activities should be assigned based on the plan defined in MP003. These resources include appropriate people resources (staff), funding, facilities, tools, techniques, and methods. As the plan is updated, the resourcing should be updated accordingly.

The phrase *people resources* refers to staff who are assigned duties to support all or a subset of activities with the [DOMAIN NAME] domain. The intent is to determine if the staff members have the appropriate knowledge, skills, and abilities to carry out their assigned [DOMAIN NAME] requirements.

Funding resources refers to the funds needed to fully execute the activities in the [DOMAIN NAME] domain, including proper oversight, execution, and maintenance of these activities. Funding is also an indication of high-level management support and sponsorship of [DOMAIN NAME] activities.

Tools refers to the specific tools required to ensure the activities in the [DOMAIN NAME] domain can be carried out as documented in the plan and procedures.

Maturity Level (ML) MP006: Review and measure [DOMAIN NAME] activities for effectiveness.

REFERENCES

• CERT RMM V1.2 GG2.GP8

DISCUSSION [CERT RMM V1.2 GG2.GP8]

Measure and control the process against the plan for performing the process and take appropriate corrective action.

The purpose of this process is to perform the direct day-to-day measurement and controlling of the process. Appropriate visibility into the process is maintained so that appropriate corrective action can be taken when necessary. Measuring and controlling the process involve establishing appropriate metrics and measuring appropriate attributes of the process or work products produced by the process. The metrics and measurements may be qualitative or quantitative as appropriate.

CLARIFICATION

The organization defines measurement criteria, measures [DOMAIN NAME] activities periodically, and evaluates the results. The [DOMAIN NAME] activities should be reviewed for effectiveness against the plan defined in MP003.

Examples of activities include:

- measurement of actual performance against the plan for performing the process
- review of accomplishments and results of the process against the plan for performing the process
- review of activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues
- identification and evaluation of the effects of significant deviations from the plan for performing the process
- identification of problems in the plan
- corrective action when requirements and objectives are not being satisfied
- corrective action tracking to closure

Maturity Level (ML) MP007: Review the status and results of [DOMAIN NAME] activities with higher level management and resolve issues.

REFERENCES

- CERT RMM V1.2 GG2.GP10

DISCUSSION [CERT RMM V1.2 GG2.GP10]

CERT RMM V1.2 GG2.GP10: Review the activities, status, and results of the process with higher level managers and resolve issues.

Higher level managers include those in the organization above the immediate level of managers responsible for the process. This information is provided to help higher level managers to provide and enforce policy for the process, as well as to perform overall guidance. In addition, higher level managers provide oversight for corrective actions to resolve issues.

CLARIFICATION

Higher level management includes those in the organization above the immediate level of management responsible for the [DOMAIN NAME] activities.

Higher level managers are informed of the status of [DOMAIN NAME] activities. When issues are identified, corrective actions are developed to resolve issues. This ensures that higher level management is given appropriate visibility into the [DOMAIN NAME] activities. This allows them to provide and enforce policy, as well as to provide overall guidance. The reviews should be both periodic and event-driven, when necessary.

Examples of reviews include:

- status reviews of [DOMAIN NAME] activities
- issues identified in process and plan reviews
- risks associated with [DOMAIN NAME] activities
- recommendations for improvement
- status of improvements being developed
- schedules for achieving milestones

Maturity Level (ML) MP008: Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units.

REFERENCES

- CERT RMM V1.2 GG3.GP1

DISCUSSION [CERT RMM V1.2 GG3.GP1]

Establish and maintain the description of a defined process.

The purpose of this process is to establish and maintain a description of the process that is tailored from the organization's set of standard processes to address the needs of a specific organizational unit or line of business. The organization should have standard processes that define the specific operational resilience management capability, along with guidelines for tailoring these processes to meet the needs of a specific organizational unit or line of business, or any other organizationally defined operating division.

CLARIFICATION

The intent of standardizing [DOMAIN NAME] is to provide consistency across the organization by defining the activities and allowing individual operating units to tailor the practices to their needs.

A standard practice may include:

- practice description
- practice activities to be performed
- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Maturity Level (ML) MP009: Share identified improvements to [DOMAIN NAME] activities across the organization.

REFERENCES

- CERT RMM V1.2 GG3.GP2

DISCUSSION [CERT RMM V1.2 GG3.GP2]

Collect work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

The purpose of this process is to collect information and work products derived from planning and performing the process. This process is performed so that the information and work products can be included in the organizational process assets and made available to those who are planning and performing the same or similar processes. The information and work products are stored according to organizational standards.

CLARIFICATION

Ensure that improvements to [DOMAIN NAME] practices are documented and shared across the organization. Documenting lessons learned during the execution and review of [DOMAIN NAME] activities facilitates the proposal of improvements to the process. Sharing lessons learned enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products include:

- process metrics and measurements
- lessons learned from process reviews
- policy violations and improvements
- relevant internal and external audit reports and resolutions

APPENDIX F: 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

Activity/Activities

Set of actions that are accomplished within a practice in order to make it successful. There can be multiple activities that make up a practice. Practices may only have one activity and some may have a set of activities.

Source: CMMC

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 the combination 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

CDI (Covered Defense Information)

Term used to identify information that requires protection under DFARS Clause 252.204-7012. Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is:

- Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR
- Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.

Source: DFARS Clause 252.204-7012

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*

Covered Defense Information (CUI)
See Glossary: CDI

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

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

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

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: D*efined 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 G: ACRONYMS

Below is a list of acronyms used in the CMMC Model Version 0.7.

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
C###	Capability number ###
CDI	Covered Defense Information
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
CTI	Controlled Technical 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