CMMC and Insider Threat Program:

Two Cohesive Eliminate Working Together to Eliminate the Threat

Presented By Jeanie Alford, CISO
OWT Global, LLC,
Information Assurance Lead, Insider Threat Subcommittee

AGENDA

- Clarify the levels of CMMC with regards to CUI
- Exhibit the need for adhering to DFARS 252.204.7012 compliance for long term CMMC requirements
- Steps to Compliance
- Increase the understanding of a well-planned Insider Threat Plan and the relevance and importance to CMMC
- Brief overview of the example CMMC controls .xml

CMMC and DFARS 252.204.701

DFARS Clause

- Implement all NIST Special Publication 800-171;conduct NIST 800-171 basic self assessment as of 29 SEP 2020
- Choose Cloud vendors according to a strict criteria (FedRAMP).
- Report cyber incidents affecting contractor networks to the DoD.
- Notify the DoD of any security not implemented, within 30 days of contract award

CMMC

- 5 Maturity levels
- Expected to be fully roled out by 2025
- Required third-party assessors to come on premise and evaluate your operating environment
- 130 controls make up level 3; level 3 builds off 1 & 2 and covers 100% of the controls in NIST 800-171 adding an additional 20.

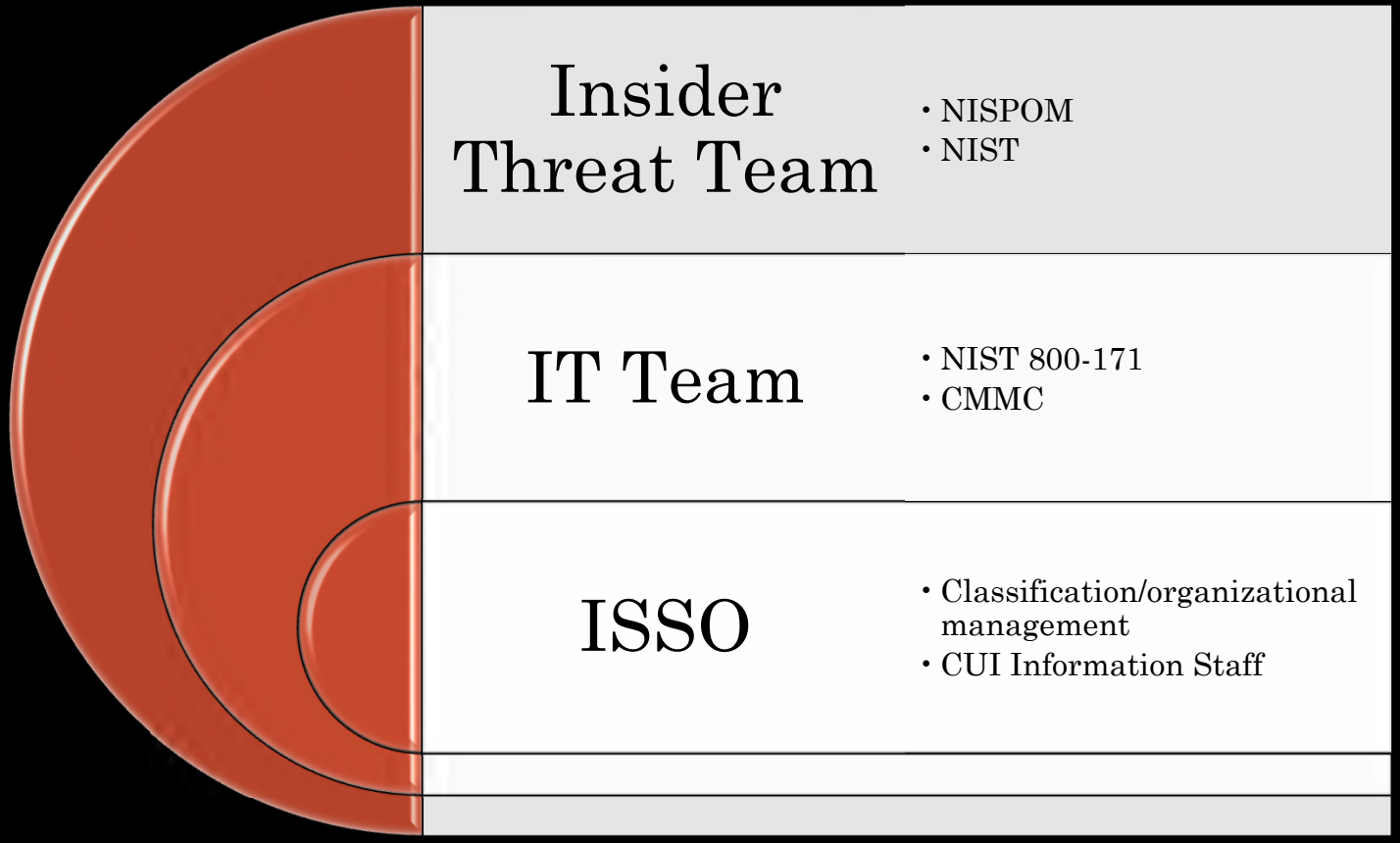
CUI Level 3

- Practices: Good cyber-Hygiene:- Level three focuses on the protection of CUI. This encompasses all the security requirements specified in NIST SP 800-171 as well as additional controls set forth in the CMMC.
- Includes the DFARS Clause: 252.204.7012:-Safeguarding Covered Defense Information and Cyber Incident Reporting
  - -Controlled defense information means unclassified controlled technical information or other information as described in the Controlled Unclassified Information (CUI) Registry here that requires safeguarding or dissemination controls pursuant to and consistent with, law, regulations, and Governmentwide policies.
- It is currently recommended that contractors and sub-contractors safeguarding CUI, implement all controls up to level three.
- The basic self-assessment covers all 110 controls within NIST800-171. Once the POAM&s are closed within the self-assessment, it is recommended organizations start to implement the CMMC controls needed to meet their organization's expectation level
- The CMMC is a maturity process; in order to achieve a level three, levels two and one must be achieved first

Steps to Achieving Compliance

- Assess current policies and procedures and how they address CUI
- Identify CUI and who needs access to it; create a flow down of where your CUI will be going
- Conduct a risk assessment/ Vulnerability assessment- starts with asset identification
- Conduct gap analysis and create POA&M to include CMMC practices
- Assess user access and least privileges accounts
- Conduct self assessments and prepare for C3PAO assessments once policies are updated and POA&Ms are closed

Insider Threat Plan and CMMC



Insider Threat and CMMC

- NISPOM defines an Insider Threat as the likelihood, risk, or potential that an insider will use his or her access, wittingly or unwittingly, to do harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protract classified national security information. (A person with authorized access to CUI that can cause harm to your organization without proper training, auditing, prevention measures, and policies).

- Insider Threat team and cybersecurity team will be instrumental in preventing an Insider attack and meeting numerous CMMC controls as they will set forth the policies for access control, awareness and training, portable media controls, multi factor authentication, and end-point protection etc.

- Using this .xml file, we can look at the CMMC controls within each level and identify how the Insider Threat plan can address it

Useful Links

DIBNet-Partner Sharing Network and Cyber Incident reporting page

Cyber Security Awareness Training for DoD and Industry

Insider Threat Awareness Training for DoD and Industry

OPSEC Awareness Training for Military Members, DoD Employees and Contractors

DoD Mandatory Controlled Unclassified Information (CUI) Training

CUI Registry for CUI Classifications

QUESTIONS/COMMENTS

Insider Threat and CMMC: Two Cohesive Elements Working Together to Eliminate the Threat

Abstract: The evolution of the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)[1] program has produced a broad range of complex starting points for defense contractors new to the subject. For industry, the most difficult part of CMMC may be determining where to start. For organizations maintaining a facility clearance, storing, transmitting, and creating controlled unclassified information (CUI), it is currently recommended that CMMC levels, 1,2 and 3 are implemented. Creating a well thought out Insider Threat Program developed by the ITPSO and the IT cybersecurity team will be instrumental in an organization's compliance success.

CMMC is a cybersecurity focused maturity program that ranges from basic hygiene to advanced levels with each level building incrementally. Of the 171 best practices described in the CMMC, a large portion of those can be addressed by the development of a NISPOM compliant Insider Threat Program, that includes NIST 800-171, compliance for CUI. The organization's cybersecurity team should play an integral part in the creation of this program. This will ensure that not only compliance in creating an Insider Threat Program will be completed, but that it will include DFARS 252.204-702 requirements as well. This program will adequately align the protection of controlled unclassified information, sensitive and proprietary organization data and ensure unauthorized individuals are prohibited from accessing CUI by implementing appropriate controls. By examining CMMC controls[2], both your Insider Threat Program Officer (ITPSO) and your Information Technology department can devise the best practices for successful compliance.

Compliance with these frameworks in addition to establishing and maintaining a well-planned Insider Threat Program is necessary for your organization's continued participation in the National Industrial Security Program (NISP)[3].

It is estimated by 2025 that, all DIB[4] contractors must achieve a level of CMMC compliance,[5] successfully complete an audit and receive a certificate before they are awarded a DoD contract. Similarly, to the Insider Threat Program development, the first step to CMMC compliance is a self-assessment to identify the gaps. Through the self-assessment, one will likely identify that a technological control will often be followed by an administrative control or policy control. A detailed policy will assist the stakeholders to identify risks, gaps, and procedures required for the necessary implementation of safeguarding measures to protect controlled unclassified

[1] Cybersecurity Maturity Model Certification (CMMC) (osd.mil)
[2] What are Security Controls? | IBM
[3] National Industrial Security Program (NISP) (dcsa.mil)
[4] Defense Industrial Base Sector | CISA
[5] Department of Defense Contracts: Preparing for Cybersecurity Requirements - UW Research (washington.edu)

Information (CUI)[6]. Controlled Unclassified information can be anything from personally identifiable information (PII), export controlled, legal, financial, and proprietary information.

The Insider Threat Program is potentially the most significant policy for safeguarding CUI. The National Industrial Security Program Operating Manual (NISPOM) defines an Insider Threat as the likelihood, risk, or potential that an insider will use his or her access, wittingly or unwittingly, to do harm to the National security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information[7]. Thus, the connection between insider threat and CUI is a person with access to CUI and one that could cause serious harm to your organization without proper training, auditing, prevention measures, and policies. Your internal cybersecurity information technology partners will be instrumental when establishing your Insider Threat Program as they will help maintain and establish access controls, awareness training, portable media controls, multi factor authentication (MFA), and endpoint protection. The NISPOM was issued in accordance with the NISP which prescribes the requirements, restrictions, and other safeguards to prevent the unauthorized disclosure of data. Furthermore, the Information Security Oversite Office (ISSO) is responsible for implementing directives that shall be binding on agencies. The ISSO has three components, the classification management staff, the operations staff and the Controlled Unclassified Information Staff[8]. Thus, your ITPSO, will use their main regulatory guidance from the NISPOM and the IT team will use their regulatory guidance from the CMMC and the NIST 800-171 all of which tie together.

It is also important to note, the IT and HR teams will likely be a part of personnel vetting. If the contractor is maintaining a Facility Clearance, they are required to follow Defense Counterintelligence Security Agency (DCSA) policies as well.[9] The Insider Threat Program and annual Insider Threat Awareness training for all employees will be inspected annually during your organization's security vulnerability assessment and it is likely to come into effect with the future CMMC audits as well.

Where to start: on 30 November 2020, the DoD executed an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and CMMC framework to better assess contractor cybersecurity requirements and enhance the protection of CUI within the DoD supply chain.[10] The interim rule, the NIST SP 800-171 DoD assessment methodology amends the DFARS subpart 204.73, safeguarding covered defense information and cyber incident reporting ; directs contracting officers to verify in the Supplier Performance Risk System (SPRS) that their organization has a current NIST SP 800-171 DoD self- assessment on record prior to contract award. Contractors will only have to do this if they are required to implement NIST SP 800-171 pursuant to DFARS clause 252.204.7012 (safeguarding covered defense information and cyber incident reporting). This rule is expected to help contractors meet the upcoming compliance for CMMC and enhance the

---

[6] Controlled Unclassified Information (dcsa.mil)
[7] DoD 5220.22-M; February 2006; Incorporating Change 2 on May 18, 2016 (whs.mil)
[8] Information Security Oversight Office (ISOO) | National Archives
[9] Insider Threat (dcsa.mil)
[10] Federal Register :: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

protection of federal contract information and CUI within the DIB sector.[11] Using the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 dated June 24th, 2020, the cybersecurity IT partner and ITPSO can begin working on their Insider Threat Plan by identifying gaps in computer security configurations that may lead to a potential compromise. Evaluating and understanding the self-assessment guide which, lists the 110 NIST 800-171 security requirements that needs to be met to be compliant, will give you a better understanding of which ones need to be implements. Of the 110 security requirements, certain ones do have more impact on the overall security of the organization than others. For example, failure to limit access to authorized users (basic security requirement 3.1.1) renders all the other Access Control requirements ineffective. The DoD assessment methodology will allow the IT and ITPSO team to identify their security risks. Once the risks are identified, the team will then create their plan of action and milestones (POA&M) and propose dates for when those risks will be closed or mitigated. The goal of this self-assessment will be to reach compliance for all 110 NIST 900-171 controls and eventually move onto the CMMC framework's self-assessment.

The NIST 800-171 DoD has three levels of assessment, basic (contractor self-assessment), medium (DoD assessment), and high (on site or virtual assessment). For the medium and high assessments, both require reviews of the system security plan and associated policies related to the covered contractor information systems. [12] The requirements of your contract will outline which type of assessment your organization will be required to present to be awarded the contract. The organizations ITPSO and IT team will be instrumental when creating the Insider Threat Plan and the System Security Plan (SSP). The SSP will provide a complete overview of 110 NIST 800-171 security requirements of the system and describe the controls in place or planned to be put in place, the user responsibilities and expected behaviors of the induvial users. [13] The insider Threat Program addresses and analyzes information from multiple sources on concerning behaviors and any risks that could potentially harm your organization. NISPOM regulation 1-202 a. The contractor will establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, as required by the appropriate CSA.[14] Both the ITPSO and the IT team have specific requirements to gather, integrate, analyze and report suspected malicious behavior that could be indicative of an insider threat. The ability to integrate the two teams while creating both policies will streamline the risk management process and provide stakeholders with a better understanding of the security and reporting processes as well as their level of compliance.

Overall, the Council of Economic Advisors estimates malicious activity has cost the U.S. economy between $57 billion and $109 billion in 2016. Over ten- years this loss could equate to $570 billion to $1.09 trillion dollars.[15] In order to compete against the ever-evolving adversary,

---

[11] Federal Register :: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

[12] NIST SP 800-171 Assessment Methodology Version 1.2.1 6.24.2020.pdf (osd.mil)

[13] Checklists & Step-by-Step Guides | SCORE | SANS Institute

[14] DoD 5220.22-M; February 2006; Incorporating Change 2 on May 18, 2016 (whs.mil)

[15] Federal Register :: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

the DoD implemented the assessment methodology and the CMMC framework. While both frameworks seem to focus on the savvy technological controls put in place and used principally for monitoring systems and access, it is important to note that the DoD methodology's first control family is awareness and training, which one of the most critical control families of the CMMC framework. One of the most effective methods your organization will have at preventing a breach to your networks and a possible insider threat will be a vigilant and informed co-worker who is aware of the damages that such an event can cause to not only the organization but to national security. Employees should be trained to recognize the indicators of abnormal behavior that is not inline with your organization's authorized use policy for your systems as well as new and evolving techniques taken by the enemy. A well established and reinforced Insider Threat Program that addresses insider threats and boosts the positive outcomes when reporting an incident will help the company's success for compliance and prevention.

We will break down the Insider Threat requirements by each maturity level.

CMMC Model Version 1.02
18 March 2020

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.

This document provides a view of the model in spreadsheet format.
The content of this document is identical to the content of Appendix A.

PROCESS MATURITY (ML)

MATURITY CAPABILITY	PROCESSES		
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)
MC01 Improve [DOMAIN NAME] activities			

Note: The maturity processes are repeated in each domain. When being used in a specific domain, the first two characters of the identifier change from "ML" to the appropriate two-character domain identifier, while the rest of the identifier remains unchanged from what is shown above.

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C001 Establish system access requirements	AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). -MAINTAIN A LIST OF ALL PERSONEL AUTHORIZED TO USE COMPANY INFORMATION SYSTEMS		
		AC.2.006 Limit use of portable storage devices on external systems. SECURE ENDPOINT MANAGEMENT AND EMPLOYEE TRAINING ON THE DANGERS OF PORTABLE STORAGE DEVICES	

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C002 Control internal system access	AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. WORKING GROUP TO DETERMINE WHO SHOULD HAVE ACCESS TO WHAT OR WHO SHOULD WORK IN WHAT AREA	AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts. WORKING GROUP TOIDENTIFY THE PERSONS WHO'S ACCOUNTS NEED TO HAVE ELEVATED PRIVLIGES	AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. WORKING GROUP TO DETERMING THE SECURITY FUNCTIONS DO NOT HAVE THE ALOCATIONS ON ONE SOLE INDIVIDUAL
		AC.2.008 Use non-privileged accounts or roles when accessing nonsecurity functions. WORKING GROUP TO DETERMINE WHO'S ACCOUNTS NEED TO HAVE ELEVATED PRIVLIGES	AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. MONITOR SYSTEM LOGS FOR SECURITY MISCONFIGURATIONS
		AC.2.009 Limit unsuccessful logon attempts. ENSURE ENDPOINT MANAGEMENT WILL PREVENT A USER FROM LOGING IN AFTER SO MANY FAILED ATTEMPTS	

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C003 Control remote system access		AC.2.013 Monitor and control remote access sessions. WORKING GROUP TO DETERMINE HOW OFTEN TO REVIEW AUDIT LOGS FOR MONITORING THE REMOTE ACCESS AND WHAT TO DO IF THERE IS AN ANNOMOLY	

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
			AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information. WORKING GROUP TO DETERMINE WHO HAS ACCESS TO PERFORM REMOTELY EXECUTED PRIVLEGED COMMANDS,WHICH PRILEGED COMMANDS THEY CAN EXECUTE, AND WHO IS ALLOWED TO ACCESS SECURITY RELEVANT INFORMATION
C004 Limit data access to authorized users and processes	AC.1.003 Verify and control/limit connections to and use of external information systems. IDENTIFY THE USE OF EXTERNAL SYSTEMS/TRAIN ALL EMPLOYEES ON THEPOLICY REQUIREMENT OF USING PERSONAL SYSTEMS AND CONNECTING THEM TO THE ORGANIZATIONAL DATA		

DOMAIN: ASSET MANAGEMENT (AM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C005 Identify and document assets			
C006 Manage asset inventory			

DOMAIN: AUDIT AND ACCOUNTABILITY (AU)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C007 Define audit requirements		AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. CONFIGURE THE IS TO CAPTURE USER DATA FOR INFORMATION PERTENINT TO THE ORGANIZATION FOR TRACTING PURPOSES	AU.3.045 Review and update logged events. WORKING GROUP TO IDENTIFY WHICH EVENTS ARE RELEVANT TO THE SECURITY OF THE COMPANY'S SYTEMS FOR IDENTIFICATION AND LOGGING
C008 Perform auditing		AU.2.042 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. SET UP AN AUDIT LOG FOR ANNOMOLOUS ACTIVITIES	AU.3.048 Collect audit information (e.g., logs) into one or more central repositories. COLLECT AUDIT LOGS IN ONE CENTRAL STORAGE REPOSITORY IOT PREVENT ALTERATIONS IE. BLOB STORAGE OR OFF SITE STORAGE

DOMAIN: AUDIT AND ACCOUNTABILITY (AU)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C009 Identify and protect audit information			AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. BACKUP THE SERVER DAILY AND ENCRYPT THE DATA
			AU.3.050 Limit management of audit logging functionality to a subset of privileged users. WORKING GROUP TO DETERMINE THE USERS PERMITTED TO ACCESS THE AUDIT LOG

DOMAIN: AUDIT AND ACCOUNTABILITY (AU)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C010 Review and manage audit logs		AU.2.044 Review audit logs. REVIEW AUDIT LOGS PER YOUR POLICIES FOR REPORTING PURPOSES	

DOMAIN: AWARENESS AND TRAINING (AT)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C011 Conduct security awareness activities		AT.2.056 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. DETERMINE THE CONTTENT OF SECURITY AWARENESS TRAINING BASED ON THE ORGANIZATIONS REQUIREMENTS EX.CDSE ONLINE TRAINING	AT.3.058 Provide security awareness training on recognizing and reporting potential indicators of insider threat. DETERMINE THE CONTENT OF THE INSIDER THREAT SECURITY AWARENESS TRAINING BASED ON THE ORGANIZATIONS REQUIREMENTS

DOMAIN: AWARENESS AND TRAINING (AT)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C012 Conduct training			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C013 Establish configuration baselines			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C014 Perform configuration and change management			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)

DOMAIN: IDENTIFICATION AND AUTHENTICATION (IA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C015 Grant access to authenticated entities			

DOMAIN: IDENTIFICATION AND AUTHENTICATION (IA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C016 Plan incident response		IR.2.092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. DETERMINE AN IRPQHICH OUTLINES THE REQUIREMENTS FOR HANDELING INCIDENTS INVOLVING CUI/INSIDER THREAT	
C017 Detect and report events		IR.2.093 Detect and report events. WHEN THE IT TEAM IDENTIFIES A THREAT THEY NOTIFY THE ITPSO	
		IR.2.094 Analyze and triage events to support event resolution and incident declaration. ANALYZE EVENTS WITH THE ITPSO TO DETERMINE THE NEXT STEPS	

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C018 Develop and implement a response to a declared incident		IR.2.096 Develop and implement responses to declared incidents according to pre-defined procedures. DETERMINE THE ORGANIZATIONS RESPONSE TO INCIDENTS EXAMPLE: TRAINING USERS NOT TO CLICK ON PHISHING EMAILS	IR.3.098 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. MAINTAIN A RECORD OF INCIDENTS REPORTED EXAMPLE: INCIDENTS REPORTED TO THE DCSA
C019 Perform post incident reviews			

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C020 Test incident response			IR.3.099 Test the organizational incident response capability. TABLE TOP EXERCISES TO INCLUDE SENDING OUT FAKE PHISHING EMAILS OR COLD CALLING EMPLOYEES ASKING HOW THEY REPORT AN INSIDER THREAT

DOMAIN: MAINTENANCE (MA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C021 Manage maintenance			

DOMAIN: MAINTENANCE (MA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
		MA.2.114 Supervise the maintenance activities of personnel without required access authorization. ESCORT ALL UNKNOWN PERSONEL WORKING ON INFORMATION SYSTEMS	

DOMAIN: MEDIA PROTECTION (MP)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C022 Identify and mark media			
C023 Protect and control media			
		MP.2.120 Limit access to CUI on system media to authorized users. DETERMINE WHO THE AUTHORIZED USERS ARE	
		MP.2.121 Control the use of removable media on system components. ENDPOINT MANAGEMENT AND TRAIN USERS ON WHAT TYPES OF REMOVABLE MEDIA IS ALLOWED TO BE USED	

DOMAIN: MEDIA PROTECTION (MP)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C024 Sanitize media			
C025 Protect media during transport			

DOMAIN: PERSONNEL SECURITY (PS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C026 Screen personnel		PS.2.127 Screen individuals prior to authorizing access to organizational systems containing CUI. HAVE A SYTEM IN PLACE PER YOUR OGRANIZATION'S NEED EXAMPLE: YOUR COMPANY CONDUCTS A STANDARD CRIMINAL BACKGROUND CHECK ON A NEW EMPLOYEE			
C027 Protect CUI during personnel actions		PS.2.128 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. DETERMINE THE BEST WAY TO REMOVE AN EMPLOYEES ACCESS TO CUI DURING TERMINATION AND TRANSFER:EXAMPLE REMOVING ACCESS TO CUI FOLDERS OR TURNING IN THEIR COMPUTER			

DOMAIN: PHYSICAL PROTECTION (PE)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C028 Limit physical access	PE.1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. DETERMINE WHO NEEDS ACCESS TO SPECIFIC OPERATING EVIRONMENTS WITHIN THE ORGANIZATION	PE.2.135 Protect and monitor the physical facility and support infrastructure for organizational systems. SECURE YOUR ORGANIZATION SYSTEMS USING ALARMS,SECURE LOCKS, DOORS, ETC.	PE.3.136 Enforce safeguarding measures for CUI at alternate work sites. PROVIDE GUIDANCE AND TRAINING TO USERS ON ENTERPRISE SECURTY WHEN WORKING AT ALTERNATE LOCATIONS
	PE.1.132 Escort visitors and monitor visitor activity.		
	PE.1.133 Maintain audit logs of physical access. HAVE A CHECKLIST BY YOUR FRONT DOOR/SENSITIVE AREAS		
	PE.1.134 Control and manage physical access devices. HAVE A LOG OR INVENTORY KEYS,BADGES ETC.		

DOMAIN: RECOVERY (RE)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C029 Manage backups			
		RE.2.138 Protect the confidentiality of backup CUI at storage locations. MANAGE WHO HAS ACCESS TO THE RECOVERY, ENCRYPT ALL BACKUPS	
C030 Manage information security continuity			

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C031 Identify and evaluate risk		RM.2.141 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 CUI. ASSESS THE RISKS ASSOCIATED WITH HAVING CUI WITHIN YOUR ORGANIZATION, TALKING ABOUT RISKS CAN BE INFORMAL WITH STAKEHOLDERS OR A FORMAL DOCUMENTAION	

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C032 Manage risk			

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C033 Manage supply chain risk			

DOMAIN: SECURITY ASSESSMENT (CA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C034 Develop and manage a system security plan		CA.2.157 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. DEVELOP YOUR SSP TO INCLUDE ALL OF THE NIST 800-171 CONTROLS AND IDENIFY YOUR GAPS	
C035 Define and manage controls			
		CA.2.159 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	

DOMAIN: SECURITY ASSESSMENT (CA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C036 Perform code reviews			

DOMAIN: SITUATIONAL AWARENESS (SA)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C037 Implement threat monitoring			SA.3.169 Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. A COMPANY'S IT/ITPSO CAN SIGN UP FOR NCMS/DIBNet TO GAIN BETTER INSIGNT INTO BOTH CYBER INCIDENTS AND INSIDER THREATS

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C038 Define security requirements for systems and communications			

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C039 Control communications at system boundaries			

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
			SC.3.193 Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter). CREATE A POLICY AND TRAIN EMPLOYEES

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C040 Identify and manage information system flaws		SI.2.214 Monitor system security alerts and advisories and take action in response. DETERMINE HOW OFTEN AND WHEN TO MONITOR SYSTEM SECURITY ALERTS EXAMPLE: ONCE A WEEK AND CREATE AN APPLICABLE LIST OF ALERTS TO REPORT TO SECURITY TEAM	
C041 Identify malicious content	SI.1.211 Provide protection from malicious code at appropriate locations within organizational information systems. DETERMINE THE BEST ANTI-MALWARE SOLUTION FOR YOUR COMPANY		
	SI.1.212 Update malicious code protection mechanisms when new releases are available. PERFORM SOFTWARE UPDATES FOR YOUR ANTI-MALWARE WHEN NECESSARY		

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C042 Perform network and system monitoring		SI.2.216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. DEVELOP A METHODOLODY OF DETERMINING THE TYPES OF ATTACKS AND INDICATORS OF AN ATTACKS THAT NEED TO BE REPORTED WHEN MONITORING A SYSTEM;EMPLOY A MONITORING DEVICE WITHIN THE IS TO COLLECT INFORMATION I.E. SOFTWARE THAT LOGS AUDIT INFORMATION	

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
		SI.2.217 Identify unauthorized use of organizational systems. INTRUSION DETECTION SYSTEMS/TRAINING AND AWARENESS/AUDIT RECORDS	
C043 Implement advanced email protections			