Federal Help for Small DoD Contractors – MEP and APEX Accelerator Support Roles in DFARS Cybersecurity

Abstract: A large majority of the small federal contractors working for the DoD are not in compliance with DFARS 252.204-7012 cybersecurity requirements. The contractors cite cost and comprehension issues preventing compliance. These problems are leading to the leakage of protected information to our enemies and a major loss of small DoD contractors.

A solution to this problem combines specialized small contractor compliance software with technical support from both the DoD Apex Accelerators and the NIST Manufacturing Extension Partnerships (MEPs).

DFARS Cybersecurity Overview: DFARS Cybersecurity in FY 2024 requires any contractor handling Controlled Unclassified Information or CUI to prepare a System Security Plan or SSP that addresses the 110 requirements of NIST 800-171 rev. 2. Any requirements not yet implemented must be scheduled in a Plan of Actions and Milestones or POAM.

Problems for Small DoD Contractors: Although DFARS 252.204-7012 can be found in most DoD contracts written since 2018, there are no exceptions for small contractors. This is a tremendous problem for the 74% of small federal contractors under 15 staff. The median federal fabricator has 7 staff.

As one of our early DFARS 252.204-7012 Cybersecurity clients put it:

> "What is probably obvious to everyone is that meeting requirements like this is extremely onerous for small companies…I can't speak for everyone, but I would label the probability of success for the "go-it-alone option" as being zero. And both the real and opportunity costs would be staggering for a small company."

Since the young lady providing the quote had just been awarded hundreds of thousands of dollars by the DoD Small Business Innovation Research (SBIR) program, her statement reveals the problems that face even exceptional technical people confronting administrative challenges.

Proposed Solution: The ACR 2 Cybersecurity Risk Management System (ACRMS™) was developed from banking technology. The initial DFARS use was in cybersecuring 44 small Air Force SBIR awardees, with an average size of 9.6 staff per site. All 44 were able to comply with DFARS 252.204-7012, typically within 30 hours over 5 days.

The SBIR Project Manager stated that "In our role as an Air Force Partnership Intermediary, we were tasked with working with industry partners to provide technology transition assistance to multiple vendors in the Air Force SBIR program…we found that the ACR 2 Cybersecurity Risk Management System™ suits our needs and the needs of the AF SBIR companies we support."

The ACRMS™ provides a rapid turnkey program to bring small contractors into initial DFARS compliance rapidly and affordably. As Puerto Rico MEP PRiMEX noted, "This tool includes everything needed to make a company compliant in a short amount of time and at a cost that is accessible to even the smallest size businesses."

ACRMS Limitations: The ACRMS™ program was developed for small DoD contractors. This allows it to make a number of simplifying assumptions. The draft policies in the ACRMS™ policy templates are based on a 15-person fabricator (Appendix B) and would not work for a 500 -person contractor. While our price list (Appendix D) allows sites to have up to 50 staff handling CUI, most of our clients have 5-15 staff. Larger clients are encouraged to contract for additional hours of consulting, to assist in modifying the template small site policies.

Long Term Cybersecurity Compliance: SSPs scored using the NIST procedure can have scores between 110 and -203. Initial scores for small contractors are typically low, in the range of -10 to -40. Contractors are now being asked to implement safety controls that were not previously required. In our experience, going from an initial score of -40 to a more respectable score of 70-110 takes 6-12 months if technical support is available.

Federal Contractor Support: NIST Manufacturing Extension Partnerships (MEPs) and DoD APEX Accelerators (APEX) both provide technical support to small federal contractors. However, typically their areas of expertise and modes of operation are different.

MEP organizations focus on technology implementations, and some will only work with manufacturers. APEX organizations have significant administrative expertise and are happy to work with any organization. APEX services are typically free to the users, while MEP services are subsidized. A typical MEP arrangement is 1/3 federally subsidized, 1/3 state subsidized and 1/3 paid by the end-user organization.

DFARS cybersecurity requirements have both technical and administrative components. Appendix A contains a spreadsheet showing a detailed breakdown of the 110 DFARS 252.204-7012 requirements into 4 categories;

Administrative – 69 items typically within the expertise of an APEX Accelerator. 174 points.
Lite Technical – 15 items typically handled by either an APEX or MEP organization. 55 pts.
Technical – 22 items typically within MEP expertise but not APEX. 68 points.
Specialty – 4 unusual items typically requiring outside assistance. 16 points.

Different MEP and APEX organizations will often have different skill sets. For example, MEPs in Texas, Georgia and Puerto Rico have specific cybersecurity expertise. Other MEPs have been known to reach out to Texas or Georgia for support.

A big advantage to working with a MEP or APEX organization is their ability to have boots on the ground and knowledge of local situations. For example, CUI 3.9.1/3.9.2 covers personnel screening, personnel transfer and personnel termination. Screening and termination law can be very different in California or New York compared to Georgia or Alabama.

Just because a safeguard is listed in Appendix A as administrative does not mean that your local APEX office can help with that requirement, or that your local MEP cannot. You need to talk to your local MEP or APEX Accelerator offices.

Once implemented, safeguards must be maintained and the maintenance activities recorded. If, for example, CUI 3.14.4/CUI 3.14.5 requiring regular anti-virus signature updates does not occur, 8 points (5+3) will be subtracted from the SSP score. If the signatures are updated but the update is not documented, the 8 points will be lost.

A recent set of over 100 audits by the Defense Contract Management Agency found that audited scores dropped an average of 116 points, often associated with a lack of documentation. Task management, scheduling and documentation is a major part of the ACRMS™ software.

Long Term Compliance Monitoring: A major advantage of the ACRMS™ is the multi-site compliance status monitoring made possible by the task management functions of the ACRMS™ Enterprise Edition.

ID	Enterprise Nickname	Hide
A	BLW1222DEMO	☐
B	BLW0926demo	☐
C	BLWdemo0815	☐
E	BLW0613DEMO	☐
F	BLW2021update	☐
G	Estrada	☐
H	BLW July 2023	☑
I	BLWdemo102422	☐
J	BLWdemo0919	☐

ID	A	B	C	E	F	G	I	J
Date	09/06/23	07/31/23	08/19/22	07/05/22	02/24/23	07/28/22	09/04/23	09/23/22
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	1	50	50	50	50	50	50	50
E2	1	50	50	25	50	50	25	50
E3	1	50	50	25	50	50	25	50
E4	1	50	50	50	50	50	50	50
E5	1	50	50	50	50	50	50	50
E6	1	100	100	50	100	100	50	100
HE1	1	100	50	100	100	100	100	100
HE2	1	100	50	100	100	100	100	100
HE3	1	100	50	100	100	100	100	100
HE4	1	100	50	100	100	100	100	100
HE5	1	100	100	100	100	100	100	100
HE6	1	25	25	25	50	50	50	50
HE7	1	100	100	100	100	100	100	100
HE8	1	50	50	50	100	100	100	100
MI1	1	100	100	100	100	100	100	100
MI2	1	100	100	100	100	100	100	100
MI3	1	100	100	100	100	100	100	100
MI4	1	100	100	100	100	100	100	100
MI5	1	100	100	100	100	100	100	100
MI6	1	25	25	50	100	100	100	100
MI7	1	25	25	50	50	100	50	100
MI8	1	25	25	50	50	100	50	100
MO1	1	25	25	25	100	50	25	25
MO2	1	25	25	25	100	50	25	25
MO3	1	25	25	25	100	50	25	25
MO4	1	50	50	50	100	50	50	50
MO5	1	25	25	25	100	50	50	50
MO6	1	5	5	25	100	100	100	100
MO7	1	5	5	50	100	100	100	100
MO8	1	5	5	50	100	100	100	100
DS	78	-26	-39	-66	-149	-188	-118	-124

A past ACRMS™ medical client was able to manage HIPAA cybersecurity for 103 locations from a single site near Detroit. A demonstration site involving only fictional data is available at www.cybercomplianceinthecloud.com , Login as BLW2023ENT for both the username and password. Interested parties are invited to experiment.

A copy of one of the available reports is shown on the right.

NIST 800-171 Rev 3 Independent Assessment: NIST 800-171 rev 3 is scheduled to be implemented in January 2024. A section of the draft is quoted below.

> **3.12.5. Independent Assessment**
>
> Use independent assessors or assessment teams to assess controls.
>
> **DISCUSSION**
>
> Independent assessors or assessment teams are individuals or groups who conduct impartial security assessments of the system. Impartiality means that assessors are free from perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the system under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations that acquire their services.

In many ways the APEX Accelerators are uniquely placed to provide a true independent assessment of contractor cybersecurity. Both MEPs and CMMC assessors are paid by the contractors being assessed, creating a conflict of interest.

Appendices: Appendices A, B, C and D are attached to this document. Appendix A summarizes the 110 requirements of NIST 800-171, dividing them into Administrative, Lite Technical, Technical and Specialty.

The 110 requirements of NIST 800-171 are organized into 87 groups in 800-171 Appendix D. NIST 800-171 requirements are cross-walked with NIST 800-53 and ISO 9000 safety controls.

Appendix B describes a composite DoD contractor based on the last 50 clients cybersecured by ACR 2 Solutions. The composite, labeled “Bobby Lee Welding” is a 15-person welding shop with two remote 1-person offices.

Appendix C includes 4 of the 87 policy templates, one template each for Administrative, Lite Technical, Technical and Specialty. CUI 3.9.1/3.9.2 (video)covers personnel screenings, personnel termination and personnel transfer. APEX Accelerator offices should have the state specific expertise to handle such issues.

CUI 3.4.6 (video) on least functionality is designated as lite or user-level technology. Either MEP or APEX offices should be able to advise on this policy, at least for small organizations. CUI 3.7.4 (video) on maintenance tools is venturing into more technical issues likely to be more appropriate for an MEP. Finally, CUI 3.11.2 (video) vulnerability scanning is typically supported by specialized outside consultants.

Appendix D is a current price list for ACRMS software and services.

MEP or APEX offices that choose to undertake the free ACRMS training will receive a full set of templates, updated as needed, a free ACRMS user account and a free ACRMS Enterprise account. The 4 hour training course, developed with the help of the Puerto Rico MEP PRiMEX, will give MEP or APEX consultants the tools and training they need to support small DoD contractor organizations.

Appendix A

800-171 Form	800-53 Safeguard	NIST 800-53 Safeguard Title	Admin.	Lite Tech.	Tech.	Specialist	Comments
	AC-2	Account Management					
3.1.1, 3.1.2	AC-03	Access Enforcement		10			Assume small business
	AC-17	Remote Access					No remote access
3.1.3	AC-04	Information Flow Enforcement		1			by policy
3.1.4	AC-05	Separation of Duties	1				
	AC-06	Least Privilege					
3.1.5	AC-06(1)	Least Privilege - Authorize Access to Security Functions	3				
	AC-06(5)	Least Privilege - Privileged Accounts					
3.1.6	AC-06(2)	Least Privilege - Non-Privileged Access for Nonsecurity Functions	1				
3.1.7	AC-06(9)	Least Privilege - Auditing Use of Privileged Functions	1				
	AC-06(10)	Least Privilege - Prohibit Non-Privileged Users From Executing Privileged Functions					
3.1.8	AC-07	Unsuccessful Logon Attempts		1			
				1			
3.1.9	AC-08	System Use Notification					
3.1.10	AC-11	Session Lock		1			
	AC-11(1)	Session Lock - Pattern-Hiding Displays					
3.1.11	AC-12	Session Termination		1			
3.1.12	AC-17(1)	Remote Access - Automated Monitoring / Control	5				No remote access
3.1.13	AC-17(2)	Remote Access - Protection of Confidentiality / Integrity Using Encryption	5				No remote access
3.1.14	AC-17(3)	Remote Access - Managed Access Control Points	1				No remote access
3.1.15	AC-17(4)	Remote Access - Privileged Commands / Access	1				No remote access
3.1.16	AC-18	Wireless Access	5				No wireless access
3.1.17	AC-18(1)	Wireless Access - Authentication and Encryption	5				No wireless access
3.1.18	AC-19	Access Control for Mobile Devices		5			
3.1.19	AC-19(5)	Access Control for Mobile Devices - Full Device / Container-Based Encryption		3			Typically bitlocker
3.1.20	AC-20	Use of External Information Systems	1				
	AC-20(1)	Use of External Information Systems - Limits on Authorized Use					
3.1.21	AC-20(2)	Use of External Information Systems - Portable Storage Devices	1				prohibition
3.1.22	AC-22	Publicly Accessible Content	1				
3.2.1, 3.2.2	AT-02	Security Awareness Training	10				
	AT-03	Role Based Security Training					
3.2.3	AT-2(2)	Security Awareness Training Insider Threat	1				
3.3.1, 3.3.2	AU-02	Auditable Events					
	AU-03	Content of Audit Records					
	AU-03(1)	Content of Audit Records Additional Audit Information			8		
	AU-06	Audit Review, Analysis, and Reporting					
	AU-12	Audit Generation					
3.3.3	AU-02(3)	Audit Events Reviews and Updates	1				
3.3.4	AU-05	Response to Audit Processing Failures			1		
3.3.5	AU-06(3)	Audit Review, Analysis, and Reporting - Correlate Audit Repositories			5		
3.3.6	AU-07	Audit Reduction and Report Generation			1		
3.3.7	AU-08	Time Stamps			1		
	AU-08(1)	Time Stamps - Synchronization With Authoritative Time Source					
3.3.8	AU-09	Protection of Audit Information	1				
3.3.9	AU-09(4)	Protection of Audit Information - Access by Subset of Privileged Users	1				
3.4.1, 3.4.2	CM-02	Baseline Configuration					
	CM-06	Configuration Settings		10			Visual inspection for small systems, scanner consultant for larger sites
	CM-08	Information System Component Inventory					
	CM-08(1)	Component Inventory - Updates During Installations / Removals					
3.4.3	CM-03	Configuration Change Control	1				
3.4.4	CM-04	Security Impact Analysis	1				
3.4.5	CM-05	Access Restrictions for Change	5				
3.4.6	CM-07	Least Functionality		5			
3.4.7	CM-07(1)	Least Functionality - Periodic Review					
	CM-07(2)	Least Functionality - Prevent program execution			5		
3.4.8	CM-07(4)	Least Functionality Unauthorized Software/ Blacklisting					
	CM-07(5)	Least Functionality Authorized Software/ Whitelisting		5			
3.4.9	CM-11	User-Installed Software	1				

800-171 Form	800-53 Safeguard	NIST 800-53 Safeguard Title	Admin.	Lite Tech.	Tech.	Specialist	Comments
3.5.1, 3.5.2	IA-02	Identification and Authentication (Organizational Users)					
	IA-03	Device Authentication	10				May need APEX or MEP help in setup
	IA-05	Authenticator Management					
3.5.3	IA-02(1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts					
	IA-02(2)	Identification and Authentication (Organizational Users) - Network Access to Non-Privileged Accounts			5		
	IA-02(3)	Identification and Authentication (Organizational Users) - Local Access to Privileged Accounts					
3.5.4	IA-02(8)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts-Replay Resistant			1		
	IA-02(9)	Identification and Authentication (Organizational Users) - Network Access to Non-Privileged Accounts-Replay Resistant					
3.5.5	IA-04	Identifier Management - Reuse	1				
3.5.6	IA-04	Identifier Management - Timeout	1				
3.5.7, 3.5.8, 3.5.9, 3.5.10	IA-05(1)	Authenticator Management Password-Based Authentication	8				
3.5.11	IA-06	Authenticator Feedback	1				
3.6.1, 3.6.2	IR-02	Incident Response Training					
	IR-04	Incident Handling		10			
	IR-05	Incident Monitoring					APEX support for response assistance
	IR-06	Incident Reporting					
	IR-07	Incident Response Assistance					
3.6.3	IR-03	Incident Response Testing	1				APEX support for response testing
3.7.1, 3.7.2	MA-02	Controlled Maintenance					
	MA-03	Maintenance Tools					
	MA-03(1)	Maintenance Tools - Inspect Tools			8		
	MA-03(2)	Maintenance Tools - Inspect media					
3.7.3	MA-02	Controlled Maintenance	1				
3.7.4	MA-03(2)	Maintenance Tools			3		
3.7.5	MA-04	Nonlocal Maintenance	5				Prohibition
3.7.6	MA-05	Maintenance Personnel	1				
3.8.1, 3.8.2, 3.8.3	MP-02	Media Access					
	MP-04	Media Storage	11				
	MP-06	Media Sanitization					
3.8.4	MP-03	Media Marking	1				
3.8.5	MP-05	Media Transport	1				
3.8.6	MP-05(4)	Media Transport - Cryptographic Protection	1				Readily available in MS Office
3.8.7	MP-07	Media Use	5				
3.8.8	MP-07(1)	Media Use - Prohibit Use Without Owner	3				
3.8.9	CP-09	Information System Backup	1				FIPs validated - WD
3.9.1, 3.9.2	PS-03	Personnel Screening					
	PS-04	Personnel Termination	8				Useful APEX support for state-specific requirements
	PS-05	Personnel Transfer					
3.10.1, 3.10.2	PE-02	Physical Access Authorizations					
	PE-04	Access Control for Transmission Medium	10				
	PE-05	Access Control for Output Devices					
	PE-06	Monitoring Physical Access					
3.10.3, 3.10.4, 3.10.5	PE-03	Physical Access Control	3				
3.10.6	PE-17	Alternate Work Site	1				None used
3.11.1	RA-03	Risk Assessment	3				ACRMS automation
3.11.2	RA-05	Vulnerability Scanning				5	CISA, Outside Consultant
	RA-05(5)	Vulnerability Scanning - Privileged Access					
3.11.3	RA-05	Vulnerability Remediation			1		
3.12.1, 3.12.2, 3.12.3, 3.12.4	CA-02	Security Assessments					
	CA-05	Plan of Action and Milestones	13				
	CA-07	Continuous Monitoring					ACRMS SSP protocols and templates
	PL-2	System Security Plan					
3.13.1, 3.13.2	SC-07	Boundary Protection			10		
	SA-08	Security Engineering Principles					
3.13.3	SC-02	Application Partitioning			1		

800-171 Form	800-53 Safeguard	NIST 800-53 Safeguard Title	Admin.	Lite Tech.	Tech.	Specialist	Comments
3.13.4	SC-04	Information in Shared Resources			1		
3.13.5	SC-07	Boundary Protection			5		
3.13.6	SC-07(5)	Boundary Protection - Deny By Default / Allow By Exception			5		Initial setup
3.13.7	SC-07(7)	Boundary Protection - Prevent Split Tunneling for Remote Devices			1		
3.13.8	SC-08	Transmission Confidentiality and Integrity					
	SC-08(1)	Transmission Confidentiality and Integrity - Cryptographic or Alternate Physical Protection				3	Commercial FIPS validated UTM - Sonicwall
3.13.9	SC-10	Network Disconnect			1		
3.13.10	SC-12	Cryptographic Key Establishment and Management	1				
3.13.11	SC-13	Cryptographic Protection	5				
3.13.12	SC-15	Collaborative Computing Devices	1				Prohibition
3.13.13	SC-18	Mobile Code		1			
3.13.14	SC-19	Voice over Internet Protocol		1			
3.13.15	SC-23	Session Authenticity			5		
3.13.16	SC-28	Protection of Information at Rest	1				Bitlocker
3.14.1, 3.14.2, 3.14.3	SI-02	Flaw Remediation					
	SI-03	Malicious Code Protection	15				Commercial
	SI-05	Security Alerts, Advisories, and Directives					APEX support
3.14.4, 3.14.5	SI-03	Malicious Code Protection	8				Commercial
3.14.6	SI-04	Information System Monitoring					
	SI-04(4)	Information System Monitoring -Inbound and Outbound Communications Traffic				5	FIPS validated UTM
3.14.7	SI-04	Information System Monitoring				3	FIPS validated UTM
		SSP Points	174	55	68	16	SSP Points
		% of total SSP points	56%	18%	22%	5%	% of total SSP points

Appendix B

CUI Cybersecurity Site Data Summary

Company Name: _____Bobby Lee Welding – Prototype Design and Fabrication

Site Name and Address:_____ BLW Associates, 200 Wolf Road Hiram, GA

Point of Contact this Location: _____Bobby Lee

Contact Phone & Email: _____770-381-9229, bobbylee@blw.net_

Total number of employees at this site: _____15_____

Total number of employees with remote access to this site:_____2_____

Short Description of Business Activities:

Bobby Lee Welding (BLW) began as a simple manual welding job shop. After upgrading to computer-controlled welding units, BLW was able to enter the more lucrative business of fabricating high precision components for DOD and aerospace applications. With the purchase of ACME Design Solutions, LLC, BLW is now able to modify and produce either single examples or small lots of high precision components.

Initial Information–Where information requested is unavailable, mark "unknown".

1. Identify personel that will be available for onsite assistance for completing the risk management program. One person may fill multiple roles.

a. Bobby Lee_____Compliance Officer – able to sign and adopt policies

b. Bobby Lee_____Human Resources Manager – able to hire and train staff

c. Bobby Lee_____Operations Manager – authorized to operate physical plant

d. Tommy Lee_____IT Manager – able to install and manage data handling equipment

e. __GaMEP_____IT Consultant – resource for difficult technical issues

2. For this site, is a current Network Topology Diagram available, (Y). If yes, please attach. (Note: the free software program LibreOffice has a Visio clone drafting program that makes it simple to turn a pencil drawing into a useful diagram. A YouTube video detailing the process is at https://www.youtube.com/watch?v=4laWj95PimI)

3. List of employees:

Owner: Bobby Lee

IT Manager: Tommy Lee

Administrator: Sarah Lee

Remote workers: Brandon Lee (accountant) and Jimmie Lee (Tech Crew)

Production: Mike Evans, Matthew Evans, Luke Hunter, Chris Smith, Billy Morrison, James Tyler

Design: Cindy Wells, Johnny Hughes, Lucas Granger, George Shaw, Will George, Riley Mortar

4. Create Device Inventory of all devices connecting to the network or accessing protected information (PI) *(i.e., PCs, Smart phone, Mobile Device, etc.)* Please append Inventory to this form.

a. How many and what type of computers or servers or other devices?

i. _9_____Windows workstations with Office 365

1. 5 win 10 pro

2. 4 win 11 pro

ii. _6_____Linux, welding machine controllers

iii. _0__Mac

iv. _17__ Android phones with full device encryption and Office 365

v. _0__ iOS

5. Software Summary – major software packages

MS Office

Quickbooks

AutoCad

WeldPro

6. Network Details - Are computers part of an Active Directory domain? (Y ***/*** **N**)

7. Firewalls, including next-generations Firewalls (NGFW) and/or Intrusion detection/intrusion prevention systems (IDS, IPS)? (**Y** / N)

a. If Yes, Manufacturer / Model _____Fortinet WiFi 50_____

b. If Yes, Summarize Recent experience

Number of Days in Dataset _____30_____

Total Number of Intrusions _____4_____

Total Number of Alerts _____17_____

Total Number of Warnings _____120_____

Total Number of Virus Detections _____3_____

8. Do you allow remote access? If so, how? (Mark all that apply)

a. _X__ Virtual Private Network (VPN)
b. ___ SSH
c. ___ Terminal server
d. ___ HTTPS
e. ___ Other

9. Cloud-based servers (Y / **N**) Manufacturer / Type _____

10. Cloud-based storage (**Y** / N) Manufacturer / Type _____AWS___Gov Cloud__

11. Cloud-based applications (Software as a Service) (Y / **N**) Manufacturer / Type

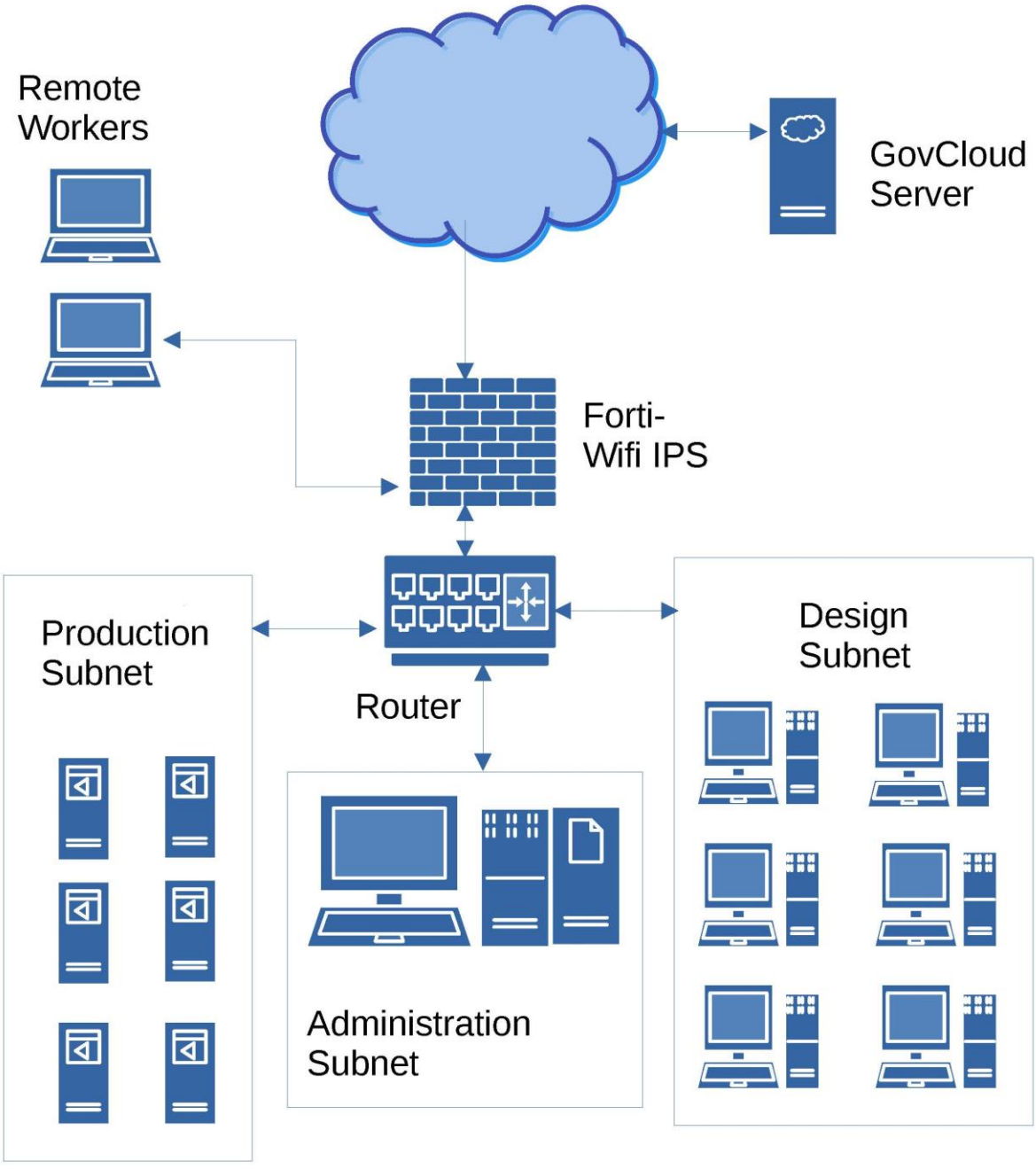
_____

12. Staff Experience

Total Number of People with Access to Protected Information ____17____

Total Number of People with Access and < 1 year Experience _____1___

Bobby Lee Welding Network Diagram



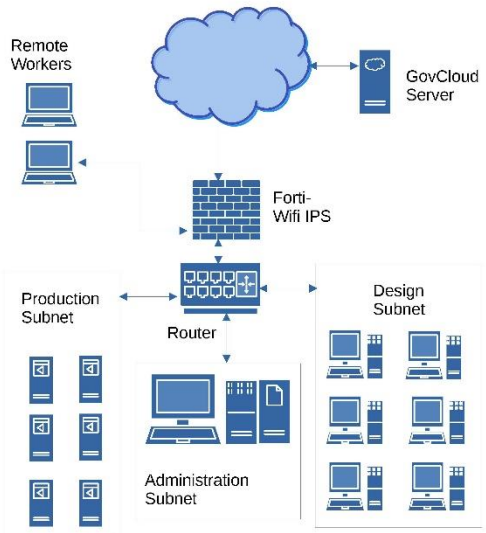
Network Security Auditing at Bobby Lee Welding

Auditing of network and computer functions is a major part of the DFARS cybersecurity program. Security auditing for the Bobby Lee Welding computer network shown at right involves two basic tasks;

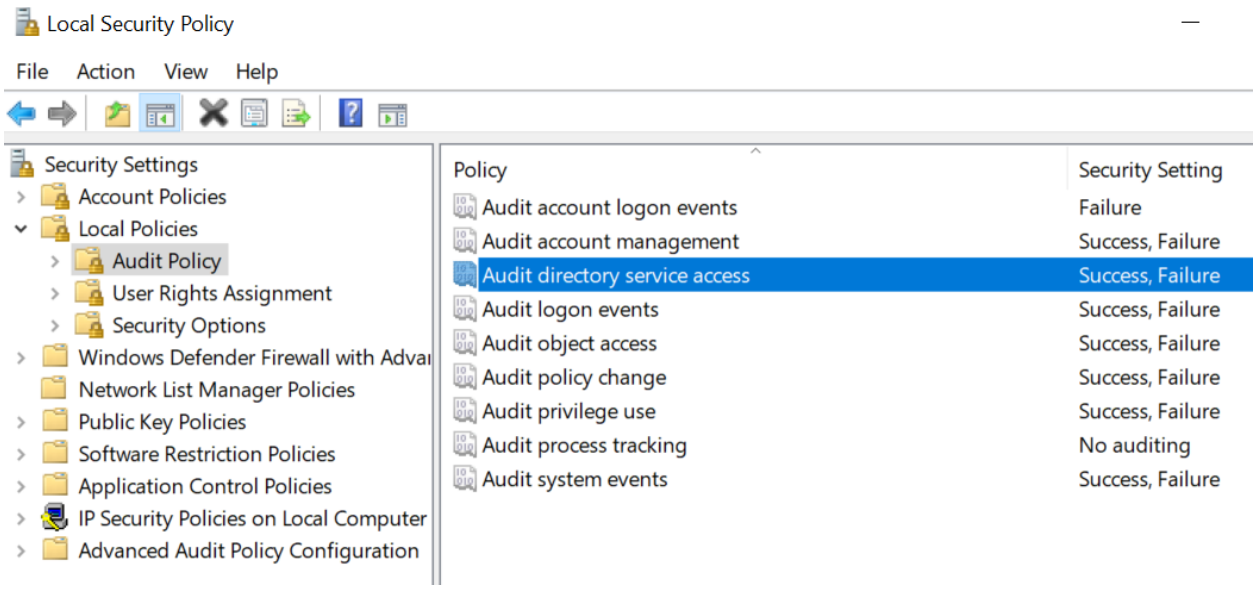
1. Perimeter monitoring using a Fortinet Unified Threat Management (UTM) device.
2. Windows™ 10 monitoring using the built in Windows™ security policy (secpol.msc) and event viewer functions (eventvwr.msc).

Perimeter monitoring is straightforward using the Fortinet reporting tools. The UTM logs attempted viruses, intrusions, warnings and alerts. This data is used as part of the ACRMS™ auto calculated NIST 800-30 risk assessment required as part of the DFARS 252.204-7012 System Security Plan (SSP).

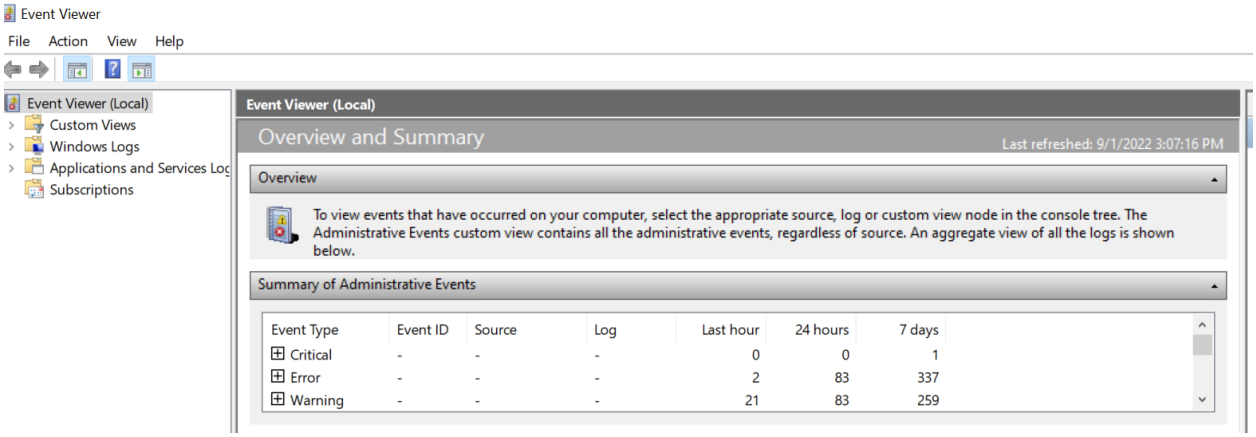
Bobby Lee Welding Network Diagram



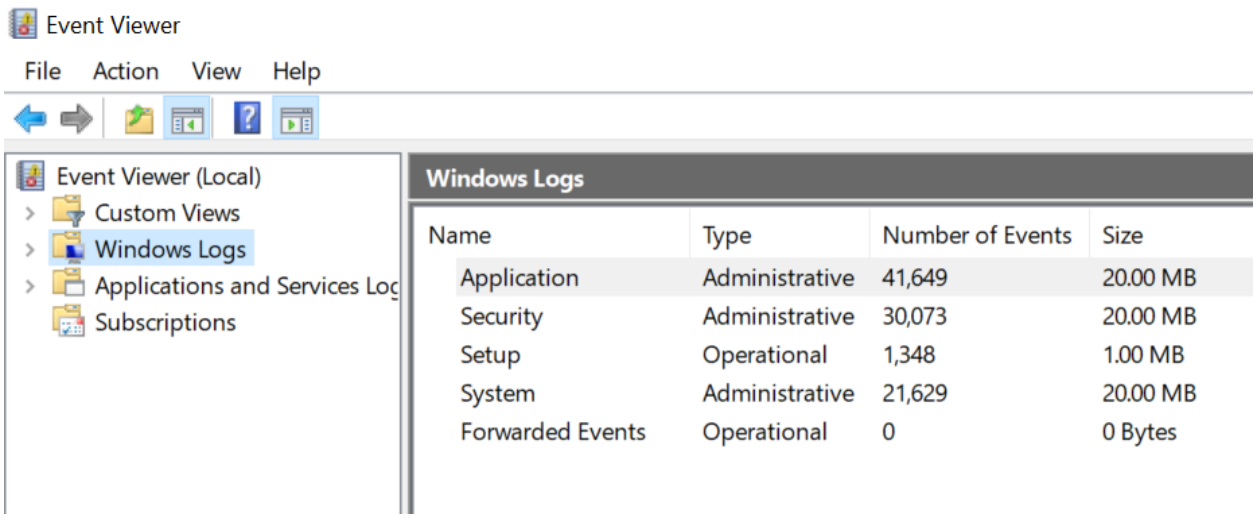
To set a security policy on a windows 10 machine click Windows™ key + R and enter secpol.msc. Clicking on "Local Policies" brings up a large number of options, as shown below. Audit Policy gives useful information about various events and functions.



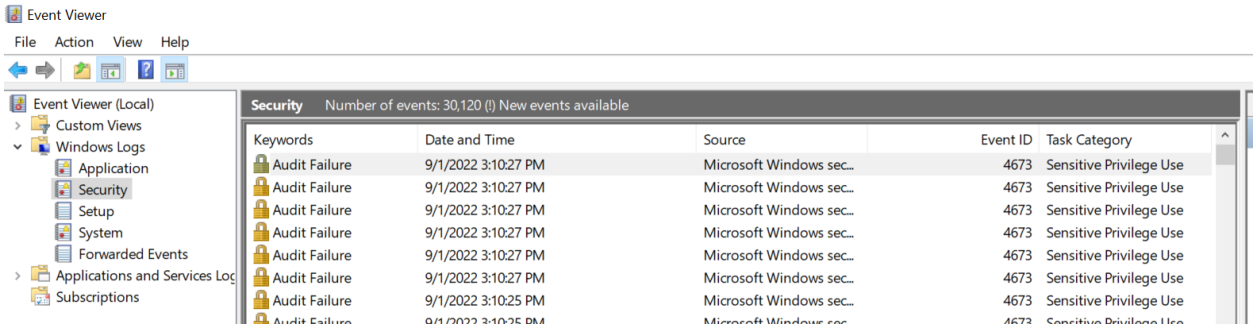
Periodic review of the audited policies is best done using the built-in Windows 10 Event Viewer. Click on Windows™ + R and enter eventvwr.msc.



Open the “Windows Logs” tab as shown below.



Typically the security logs and application logs will be of most interest.



Appendix C

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.9.1, 3.9.2

Video: https://attendee.gotowebinar.com/recording/2408325615741023759

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.1 Self-assessment Workbook Questions

1. Are individuals requiring access screened before access is granted?

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.9.2 Self-Assessment Workbook Questions

1. Does the company disable information system access prior to employee termination or transfer?
2. Does the company revoke authenticators/credentials associated with the employee upon termination or transfer within a certain time frame?(e.g.,24hours)
3. Does the company retrieve all company information system-related property from the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)
4. Does the company retain access to company information and information systems formerly controlled by the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)
5. Does the company notify the information security office and data owner of the change in authorization within a certain timeframe? (e.g., 24 hours)
6. Are electronic and physical access permissions reviewed when employees are reassigned or transferred?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguards PS-3, PS-4, PS-5

PS-3 PERSONNEL SCREENING

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening*] (typically "best practices, contract requirements, and every 5 years thereafter").

PS-4 PERSONNEL TERMINATION

Upon termination of individual employment:

a. Disable system access within [*Assignment: organization-defined time period*] (typically "prior to termination");

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [*Assignment: organization-defined information security topics*] (typically "NDA's and civil and legal consequences");

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-5 PERSONNEL TRANSFER

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [*Assignment: organization-defined transfer or reassignment actions*] (typically "transfer or reassignment actions") within [*Assignment: organization-defined time period following the formal transfer action*] (typically "24 hours");

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [*Assignment: organization-defined personnel or roles*] (typically "Management") within [*Assignment: organization-defined time period*] (typically "24 hours").

Suggested Policy Clauses

1. <Organization Name> shall screen the background of each job applicant under consideration prior to hiring.
2. Employees shall be rescreened every <five years> or whenever the job requires a higher level of security.
3. <Organization Name> shall designate a job description for each employee. These job descriptions shall be consistent between locations.
4. All job descriptions shall have an associated access and access security level.
5. Once the employee is scheduled to be terminated their access to protected information should be stopped.
6. All managers and IT staff shall be notified of the termination decision.
7. Upon termination, any issued keys are recalled. The locks should be changed depending on the nature of the end of employment or if keys cannot be found.
8. An exit interview will be conducted. This interview will remind the former employee that all information is still protected and there are civil and legal consequences to disclosing any information.

9. Any passwords need to be changed that were known to the former employee. User accounts will be suspended in this way so that any information that is needed can be recalled. This may include: (delete any items that do not apply)

a) Keyless Deadbolt protecting the Server and Storage Room
b) Common password protecting the workstations
c) Compliance Officer password
d) Account passwords (if applicable)
e) Additional items: <specify any additional items> If none, delete this item.

10. Transferred employees shall be trained to fill the security level of their job description in the new location.
11. The group reviews computer systems and building access authorizations when someone is reassigned or transferred to other positions within the group.
12. The group reissues keys, identification cards, and building passes as needed. New accounts will be set up for the person and system access adjusted.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

(Editor's note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

NIST 800-171A Assessment of Policy Effectiveness

3.9.1 ASSESSMENT OBJECTIVE Determine if, for an organizational system that processes, stores, or transmits CUI, individuals are screened prior to authorizing access to the organizational systems.

3.9.1 Potential Assessment Method and Objects SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.

3.9.2 ASSESSMENT OBJECTIVE Determine if, for an organizational system that processes, stores, or transmits CUI:

3.9.2[a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established;
3.9.2[b] system access and credentials are terminated consistent with personnel actions such as termination or transfer; and

3.9.2[c] the system is protected during and after personnel transfer actions.

3.9.2 Potential Assessment Method and Objects SELECT FROM: Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records.

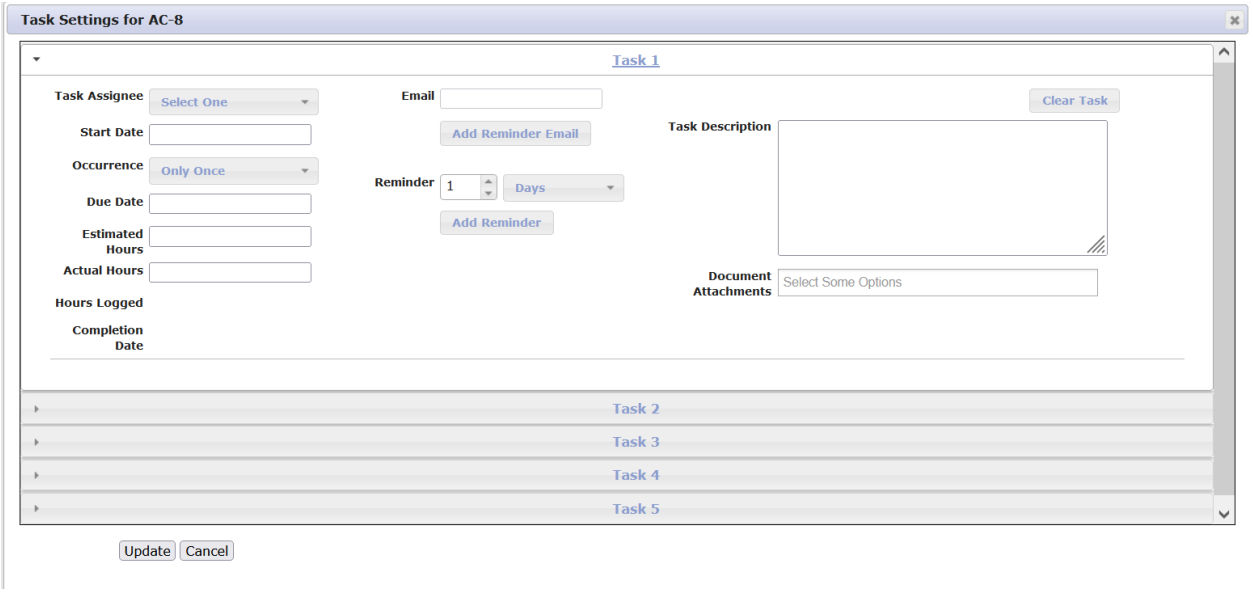
Suggested ACRMS data inputs

Screen shot of the ACRMS data input page

Question PS-3: PERSONNEL SCREENING

Answer PS-3: ☐ Yes ☐ Yes/Alt ☐ No ☐ NA ☒ Partial
Policy File PS-3: CUI 3.9.1 3.9.2 PS3 4 5 MoYr

Screen shot of the ACRMS task edit page



<Organization Name>'s <Compliance Officer> shall screen the background of each job applicant under consideration prior to hiring. File signed and dated memo in Document Management Center (DMC).

Report Example: Job Screening Memo

Bobby Lee screens each job applicant under consideration prior to hiring. Screening reports are restricted to the administration subnet. Reports are restricted to Compliance Officer, Administrative Assistant, and direct supervisor, if any.

Filename: PS-3 Job Screening Memo 08312023

Report Date: 08/31/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	--	2.00		4.00	

Estimated hours: 4

Employees shall be re-screened every <five years> or whenever the job requires a higher level of security by the <Compliance Officer>. File signed and dated report in Document Management Center (DMC).

Report Example: Re-screening Schedule

Screening reports are restricted to Compliance Officer, Administrative Assistant, and direct supervisor, if any.

Bobby Lee	06/07/2023
Tommy Lee	06/07/2023
Sarah Lee	06/07/2023
Brandon Lee	08/27/2025
Jimmie Lee	06/26/2024
Mike Evans	09/04/2025
Matthew Evans	09/04/2025
Luke Hunter	07/28/2024
Chris Smith	12/20/2024

Billy Morrison	08/04/2023
James Tyler	08/04/2023
Cindy Wells	02/08/2027
Johnny Hughes	10/10/2024
Lucas Granger	10/10/2024
George Shaw	05/04/2025
Will George	11/20/2024
Riley Mortar	02/14/2024

Filename: PS-3 Re-screening Schedule 08292023

Report Date: 08/29/2023_____
Report Author: Tommy Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Tommy Lee _____

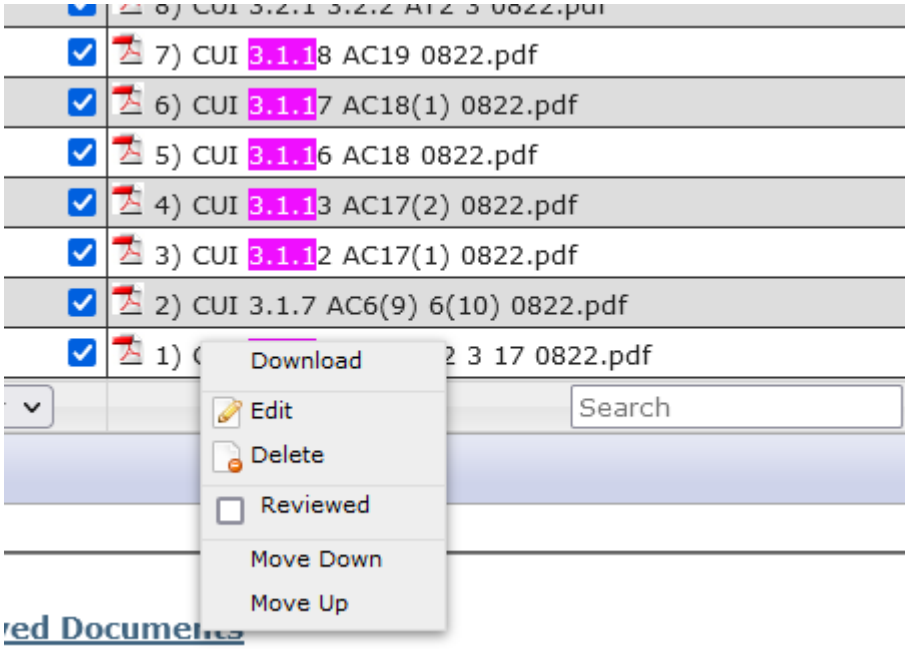
Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.50	--	0.85		1.70	

Estimated hours: 1.70

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC).

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.



Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: ___08/31/2023_____(new date)_____

Authorizing Official: _Bobby Lee___(no change)_____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.

Typed Signature: ___Bobby Lee_____(no change)__

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.10	typically only minor changes	0.10	typically only minor changes	0.10	typically only minor changes

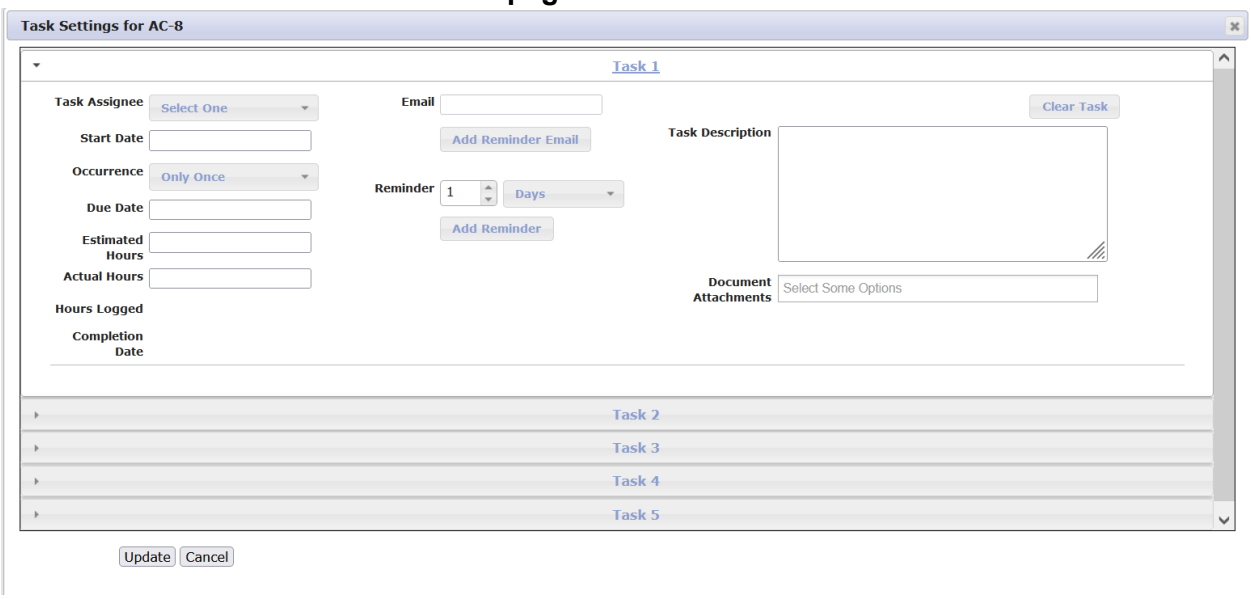
Estimated hours: 0.10

Screen shot of the ACRMS data input page

Question PS-4: PERSONNEL TERMINATION

Answer PS-4: ☐ Yes ☐ Yes/Alt ☐ No ☐ NA ☒ Partial
Policy File PS-4: CUI 3.9.1 3.9.2 PS3 4 5 MoYr

Screen shot of the ACRMS task edit page



Upon termination, any issued keys are recalled by the <Compliance Officer>. The locks should be changed depending on the nature of the end of employment or if keys cannot be found. File signed and dated memo in Document Management Center (DMC).

Report Example: Key Memo

Bobby Lee has not had to change the locks or recall keys as there have been no terminations in the last twelve months.

Filename: PS-4 Key Memo 08312023

Report Date: 08/31/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
2.00	--	4.00		8.00	1 term/yr

Estimated hours: 8

An exit interview will be conducted with the <Compliance Officer>. This interview will remind the former employee that all information is still protected and there are civil and legal consequences to disclosing any information. File signed and dated report in Document Management Center (DMC).

Report Example: Exit Interview

Bobby Lee has conducted no exit interviews in the last twelve months as there have been no terminations.

Filename: PS-4 Exit Interview 08292023

Report Date: 08/29/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	--	1.00		2.00	1 term/yr

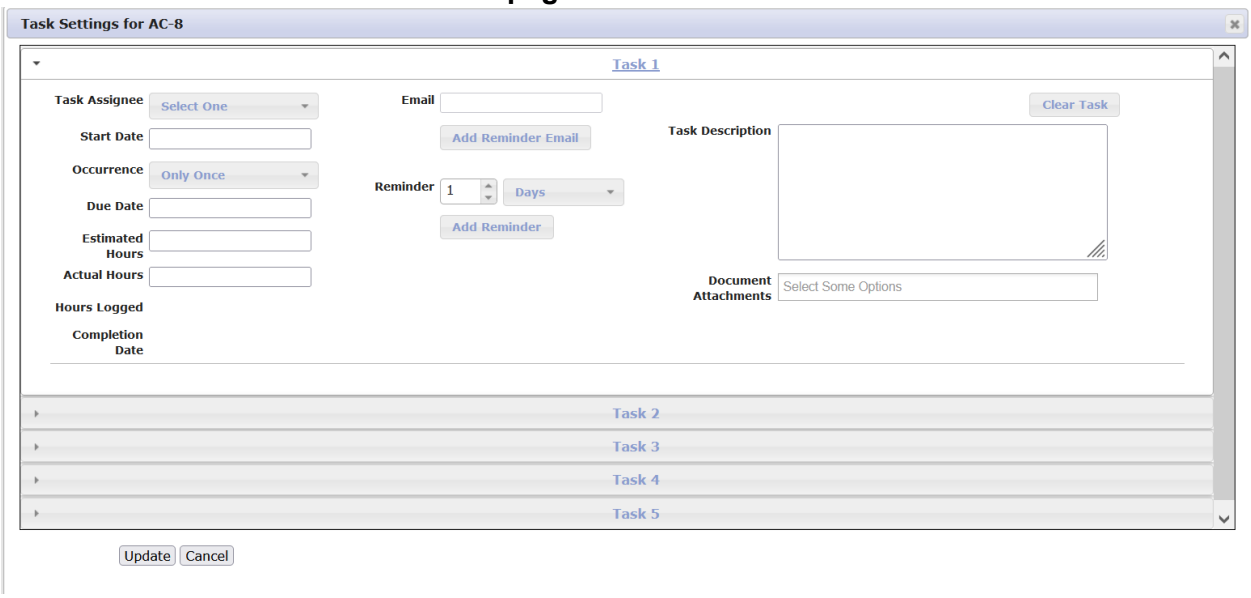
Estimated hours: 1

Screen shot of the ACRMS data input page

Question PS-5: PERSONNEL TRANSFER

Answer PS-5: ☐ Yes ☐ Yes/Alt ☐ No ☐ NA ☒ Partial
Policy File PS-5: CUI 3.9.1 3.9.2 PS3 4 5 MoYr

Screen shot of the ACRMS task edit page



<Organization Name>'s <Compliance Officer> shall designate a job description for each employee. These job descriptions shall be consistent between locations. File signed and dated report in Document Management Center (DMC).

Report Example: Job Description Summary List
Job Description Summaries:

Owner: Sales, contract management, purchasing and staff hiring and training. Also compliance Officer.

IT Manager: Purchase and install IT equipment. Audit security functions.

Administrator: Payroll and correspondence.

Accountant: Track expenditures and prepare tax returns.

Design and Tech Crew: Design prototype welded supports and devices per contract.

Production: Fabricate precision welded parts as per design.

Filename: PS-5 Job Description Summary List 08312023

Report Date: 08/31/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	--	2.00		4.00	

Estimated hours: 4

Transferred employees shall be trained to fill the security level of their job description in the new location enforced by the <Compliance Officer>. File signed and dated report in Document Management Center (DMC).

Report Example: Transfer Protocols

Bobby Lee has had no transfers in the last twelve months.

Filename: PS-5 Transfer Protocols 08312023

Report Date: 08/31/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Estimated hours: See AT-2

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.4.6

Video: https://attendee.gotowebinar.com/recording/5165774334252843536

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.6 Self-Assessment Workbook Questions

1. Is the information system configured to exclude any function not needed in the operational environment?
2. Does it deliver one function per system, where practical?
3. Does the system employ processing components that have minimal functionality and data storage (e.g., diskless nodes, thin client technologies)?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguard CM-7

CM-7 LEAST FUNCTIONALITY

a. Configure the system to provide only [*Assignment: organization-defined mission essential capabilities*] (typically “mission critical capabilities”); and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [*Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services*] (typically “see list generated by the IT Manager”).

Suggested Policy Clauses:

1. The <Compliance Officer> shall prepare a list of essential information system capabilities to meet the organization’s mission.
2. The <IT Manager> shall prepare a list of restricted functions and services for the information system.
3. The <Compliance Officer> shall approve the list of restricted functions and services for the information system.
4. All lists will be filed in the Document Management Center.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

(Editor's note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

NIST 800-171A Assessment of Policy Effectiveness

3.4.6 ASSESSMENT OBJECTIVE Determine if, for an organizational system that processes, stores, or transmits CUI:

3.4.6[a] essential system capabilities are defined based on the principle of least functionality; and
3.4.6[b] the system is configured to provide only the defined essential capabilities.

3.4.6 Potential Assessment Method and Objects SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least functionality in the system; security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

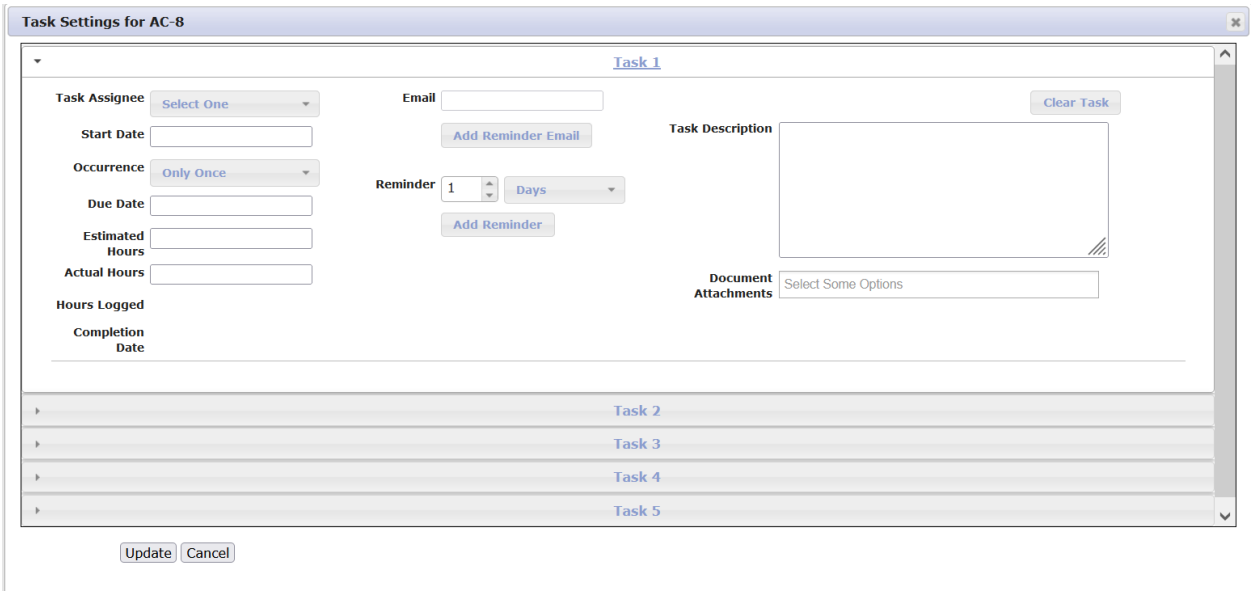
Suggested ACRMS data inputs

Screen shot of the ACRMS data input page

Question CM-7: LEAST FUNCTIONALITY

Answer CM-7: ☒ Yes ☐ Yes/Alt ☐ No ☐ NA ☐ Partial
Policy File CM-7: CUI 3.4.6 CM7 MoYr

Screen shot of the ACRMS task edit page

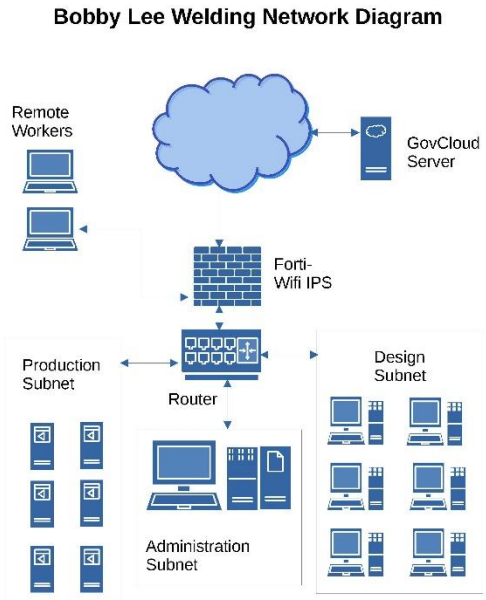


The <Compliance Officer> shall prepare a list of essential information system capabilities to meet the organization's mission. File signed and dated list in Document Management Center (DMC).

Report Example: Essential Information System Capabilities List
See document below.

Filename: CM-7 Essential Information System Capabilities List 09012023

Essential information system capabilities differ between the various subgroups of Bobby Lee Welding. As shown at right, the remote workers, design group, admin group and production group all have different tasks and different essential capabilities.



Remote workers: MS Office™, Quickbooks™, Windows™

Design group: MS Office™, Quickbooks™, Windows™, AutoCAD

Admin group: MS Office™, Quickbooks

Production group: WeldPro

Report Date: 09/01/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	memo	1.00	memo	2.00	memo

Estimated hours: 2

The <IT Manager> shall prepare a list of restricted functions and services for the information system. File signed and dated list in Document Management Center (DMC).

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	memo	1.00	memo	2.00	memo

Estimated hours: 2

The <Compliance Officer> shall approve the list of restricted functions and services for the information system. File signed and dated list in Document Management Center (DMC).

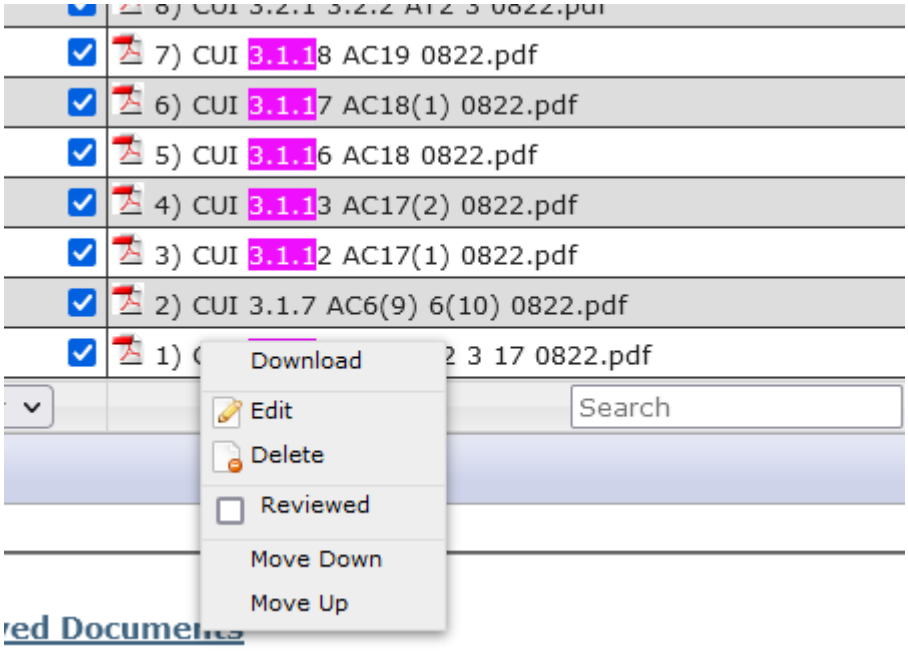
Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00		1.00		1.00	

Estimated hours: 1

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC).

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.



Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: ___09/01/2023_____(new date)_____

Authorizing Official: _Bobby Lee___(no change)_____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.

Typed Signature: ___Bobby Lee_____(no change)__

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.10	typically only minor changes	0.10	typically only minor changes	0.10	typically only minor changes

Estimated hours: 0.10

Proposed Reports Forms

1. Essential information system capabilities to meet the organization's mission.

Typical necessary information system capabilities can include the following functions.

Administration

a. Track sales and marketing activities.
b. Manage personnel.
c. Communicate with customers, suppliers, and regulators.
d. Deal with financial issues.
e. Secure data storage, both digital and physical.
f. Secure physical facilities.

Operations

a. Obtain designs and specifications.
b. Obtain raw materials.
c. Fabricate products.
d. Ship finished products to purchasers.

Much of this information can be taken from the Site Data Form, which should be filled out prior to your ACRMS™ Boot Camp.

2. List of restricted functions and services for the information system.

"Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:", often abbreviated as Ports, Protocols and Services Management (PPSM).

A useful and fairly basic discussion of this process is contained in a 2005 article from DISA located at https://www.mitre.org/sites/default/files/pdf/04_1281.pdf The DoD maintains frequently updated lists of allowed and restricted PPSM however they are not generally available except from specific contract officers. A public source is at https://www.stigviewer.com/stig/application_security_and_development/2018-04-03/finding/V-69521

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.7.4

Video: https://attendee.gotowebinar.com/recording/5568813515559182086

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.7.4 Self-Assessment Workbook Questions

1. Are media that are provided by authorized maintenance personnel (and not normal systems administrators/owners) for troubleshooting, diagnostics, or other maintenance run through an anti-virus/anti-malware/anti-spyware program prior to use in the company's information system?
2. Are the results of the scans documented in the maintenance logs?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguard MA-3(2):

MA-3(2): MAINTENANCE TOOLS: INSPECT MEDIA

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Supplemental guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Suggested Policy Clauses:

1. The <IT Manager> shall supervise all maintenance and ensure that any media containing diagnostic programs is free of malicious code.
2. The results of the malicious code scan will be included in the maintenance documentation.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

(Editor's note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

NIST 800-171A Assessment of Policy Effectiveness

3.7.4 ASSESSMENT OBJECTIVE: Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

3.7.4 Potential Assessment Method and Objects SELECT FROM: System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; security plan; other relevant documents or records.

Suggested ACRMS data inputs

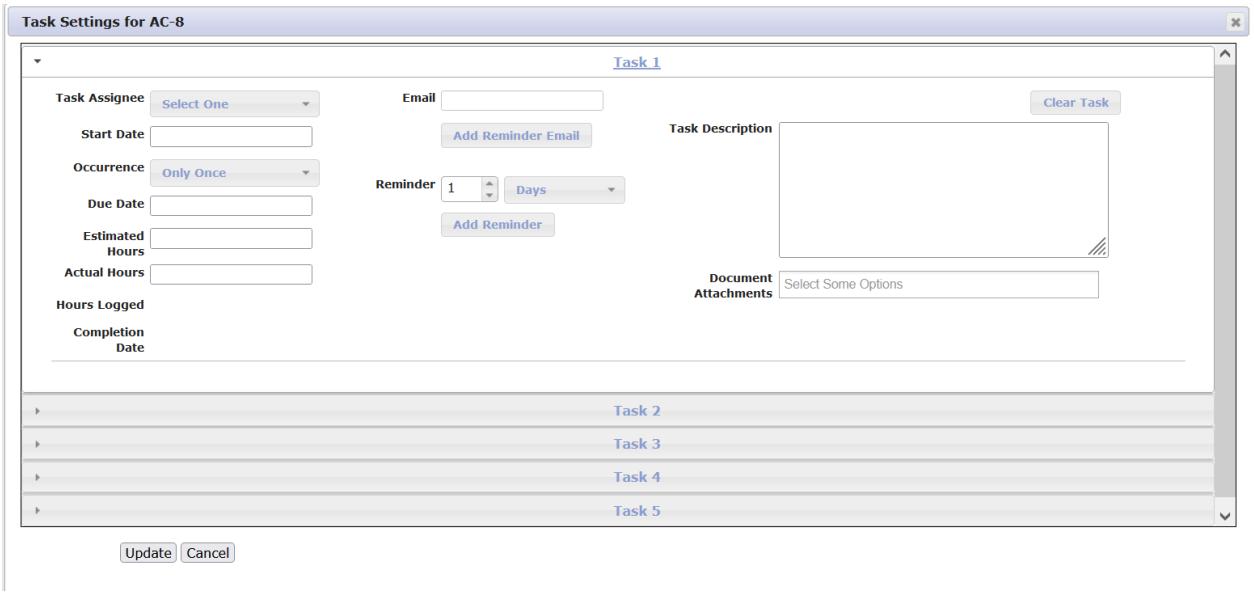
Screen shot of the ACRMS data input page

Question MA-3(2): MAINTENANCE TOOLS: INSPECT MEDIA

Answer MA-3(2): ☒ Yes ☐ Yes/Alt ☐ No ☐ NA ☐ Partial

Policy File MA-3(2): CUI 3.7.4 MA3(2) MoYr

Screen shot of the ACRMS task edit page



The results of the malicious code scan will be included in the maintenance documentation by the <IT Manager>. File signed and dated report in Document Management Center (DMC).

Report Example: Maintenance Documentation

Tommy Lee includes the results of the malicious code scan in the maintenance documentation.

Filename: MA-3(2) Maintenance Documentation 09012023

Report Date: 09/01/2023_____
Report Author: Tommy Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Tommy Lee _____

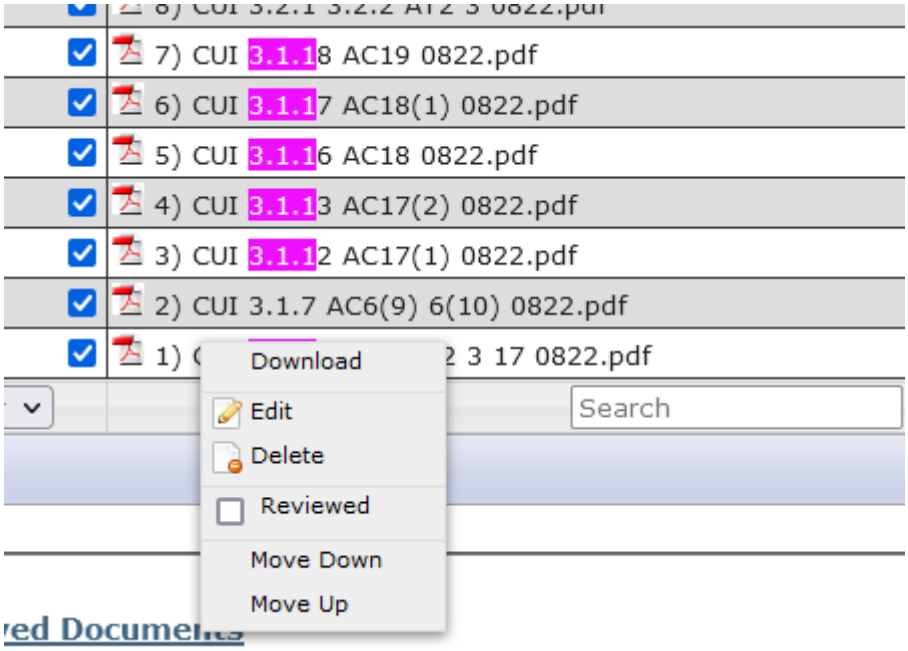
Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.50		0.50		0.50	

Estimated hours: 0.50

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC).

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.



Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: ___09/01/2023_____(new date)_____

Authorizing Official: _Bobby Lee___(no change)_____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.

Typed Signature: ___Bobby Lee_____(no change)__

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.10	typically only minor changes	0.10	typically only minor changes	0.10	typically only minor changes

Estimated hours: 0.10

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.11.2

Video Link: https://attendee.gotowebinar.com/recording/6545061100402290178

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

3.11.2 Self-Assessment Workbook Questions

1. Is vulnerability scanning performed?
2. Are systems periodically scanned for common and new vulnerabilities?
3. Are previously undocumented vulnerabilities risk assessed and documented?
4. Are reports regarding the scans made available to system owners and company management in a timely manner?
5. Are vulnerability scans performed on a defined frequency or randomly in accordance with company policy?
6. Is the list of scanned system vulnerabilities updated on a defined frequency or when new vulnerabilities are identified and reported?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguards RA-5, RA-5(5)

RA-5 VULNERABILITY MONITORING AND SCANNING

a. Monitor and scan for vulnerabilities in the system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] (typically “quarterly”) and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] (typically "within 30 days") in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] (typically "affected staff") to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 (5) VULNERABILITY MONITORING AND SCANNING | *PRIVILEGED ACCESS*

Implement privileged access authorization to [*Assignment: organization-defined system components*] (typically "the IT Manager and the Compliance Officer") for [*Assignment: organization-defined vulnerability scanning activities*] (typically "any vulnerability scanning activities").

Vulnerability Scanning Overview

Vulnerability assessments are sometimes confused with risk assessments. Page 8 of NIST Special Publication 800-30 makes the distinction clear

"Risk is a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization."

Vulnerability assessment tools have both advantages and disadvantages. An advantage is the ability to interrogate most devices on a network for vulnerabilities. A matching disadvantage is that a typical scan will reveal, literally, thousands of theoretical vulnerabilities, of which as many as 80% have never been seen in actual attacks. This can hugely divert attention from more current and more likely hazards.

Section (d) of the RA-5 safeguard notes the requirement to "Remediates **legitimate** vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational **assessment of risk**…" [*emphasis added*]. In the medical field, for example, where reporting of data breaches is required by law, some estimates indicate that up to 60% of adverse events are due to human error rather than technological circumvention of precautions. It is recommended that at least as much effort be involved in employee training as in the simpler and more entertaining vulnerability remediation.

A number of vulnerability scanners are available, especially for Windows™ workstations and servers.

Suggested Policy Clauses:

1. The organization scans for vulnerabilities in the information system <quarterly> and when significant new vulnerabilities potentially affecting the system are identified and reported.

2. Vulnerability remediation will be prioritized based on the results of <quarterly> information system risk assessments.
3. Access to the network for vulnerability scanning shall be authorized by the <Compliance Officer> and managed by the <IT Manager>.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

(Editor's note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

NIST 800-171A Assessment of Policy Effectiveness

3.11.2 ASSESSMENT OBJECTIVE Determine if, for an organizational system that processes, stores, or transmits CUI:

3.11.2[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined;
3.11.2[b] vulnerability scans are performed on organizational systems with the defined frequency;

3.11.2[c] vulnerability scans are performed on applications with the defined frequency;

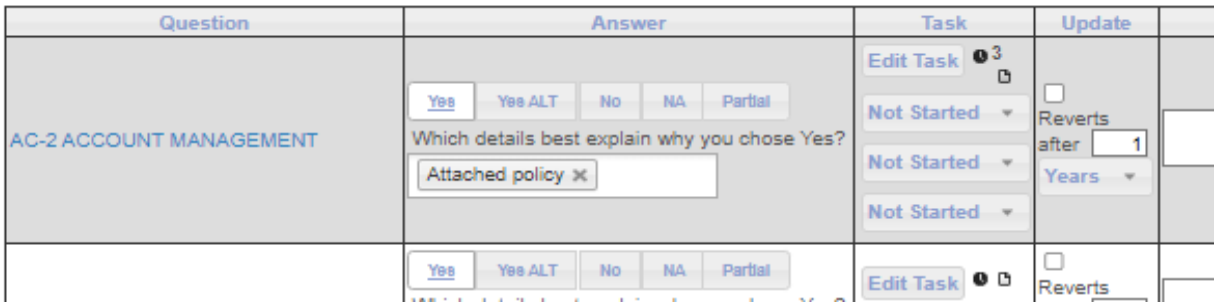
3.11.2[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified; and

3.11.2[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

3.11.2 Potential Assessment Method and Objects SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

Suggested ACRMS data inputs

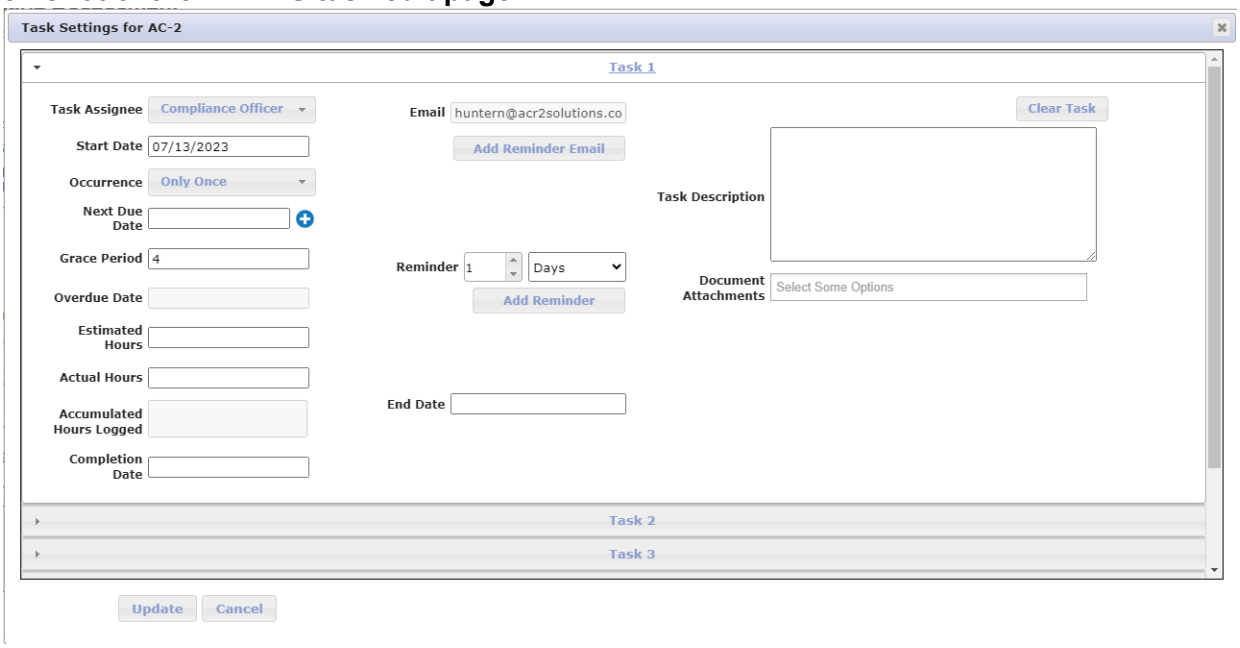
Screen shot of the ACRMS data input page



Question RA-5: VULNERABILITY SCANNING

Answer RA-5: ☐ Yes ☐ Yes/Alt ☐ No ☐ NA ☒ Partial
Policy File RA-5: CUI 3.11.2 RA5 5(5) MoYr

Screen shot of the ACRMS task edit page

The 

organization scans for vulnerabilities in the information system <quarterly> and when significant new vulnerabilities potentially affecting the system are identified and reported to the <Compliance Officer>. File signed and dated report in Document Management Center (DMC).

Report Example: Vulnerabilities List

Bobby Lee scanned for vulnerabilities in the information system quarterly and when significant new vulnerabilities potentially affecting the system are identified.
The last scan was done 06/27/2023 and the results are filed in the Document Management Center.

Filename: RA-5 Vulnerabilities List 06272023

Report Date: 06/27/2023_____
Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
3.00		6.00		12.00	

Estimated hours: 12

Vulnerability remediation will be prioritized based on the results of <quarterly> information system risk assessments by the <Compliance Officer>. File signed and dated report in Document Management Center (DMC).

Report Example: Vulnerability Remediation List

Bobby Lee prioritizes vulnerability remediation based on the results of quarterly information system risk assessments. The last Vulnerability Scan and Risk Assessment was done at the same time on 06/27/2023. Both reports are in the DMC. The planned remediation schedule was developed by the IT Manager. The monthly CM-03 planned network change report is based on this information.

Filename: RA-5 Vulnerability Remediation List 06272023

Report Date: 06/27/2023_____

Report Author: Bobby Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Bobby Lee _____

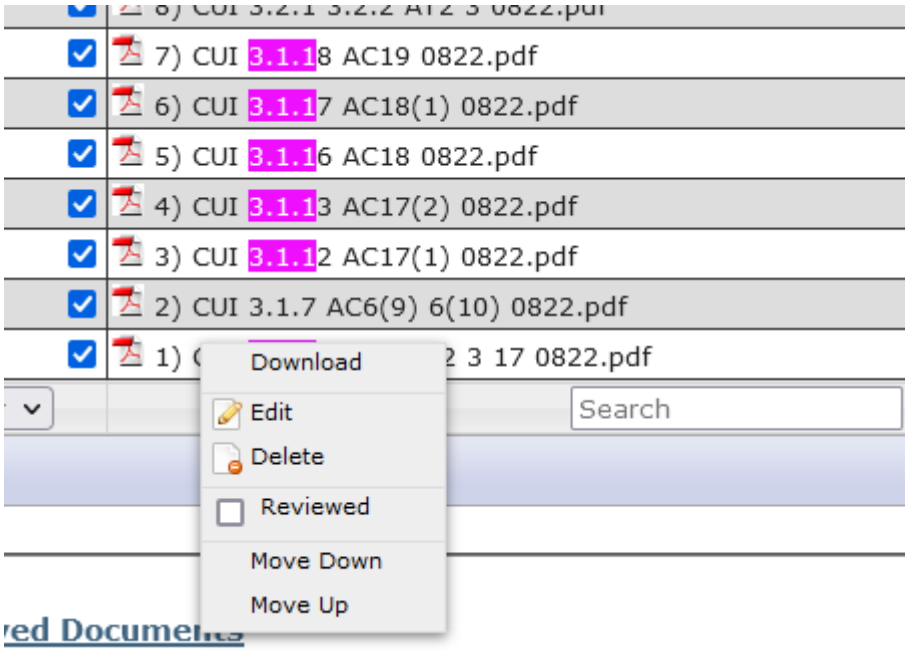
Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00		2.00		4.00	

Estimated hours: 4

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC)

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.



Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: ___09/02/2023_____(new date)_____

Authorizing Official: _Bobby Lee___(no change)_____

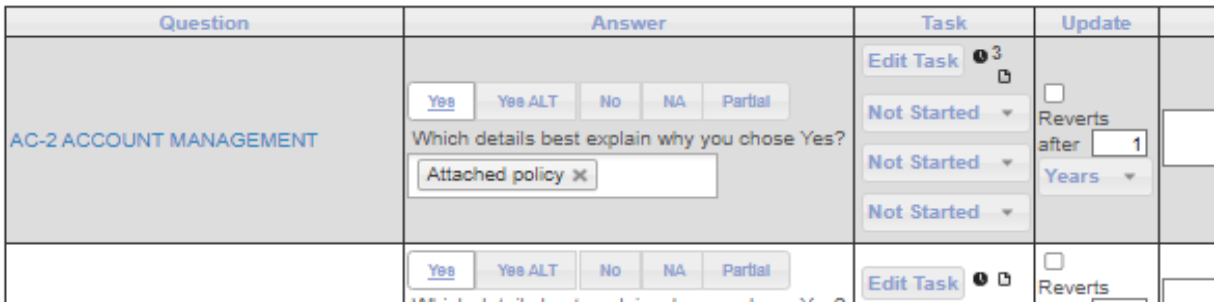
☒ Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.

Typed Signature: ___Bobby Lee_____(no change)__

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.10	typically only minor changes	0.10	typically only minor changes	0.10	typically only minor changes

Estimated hours: 0.10

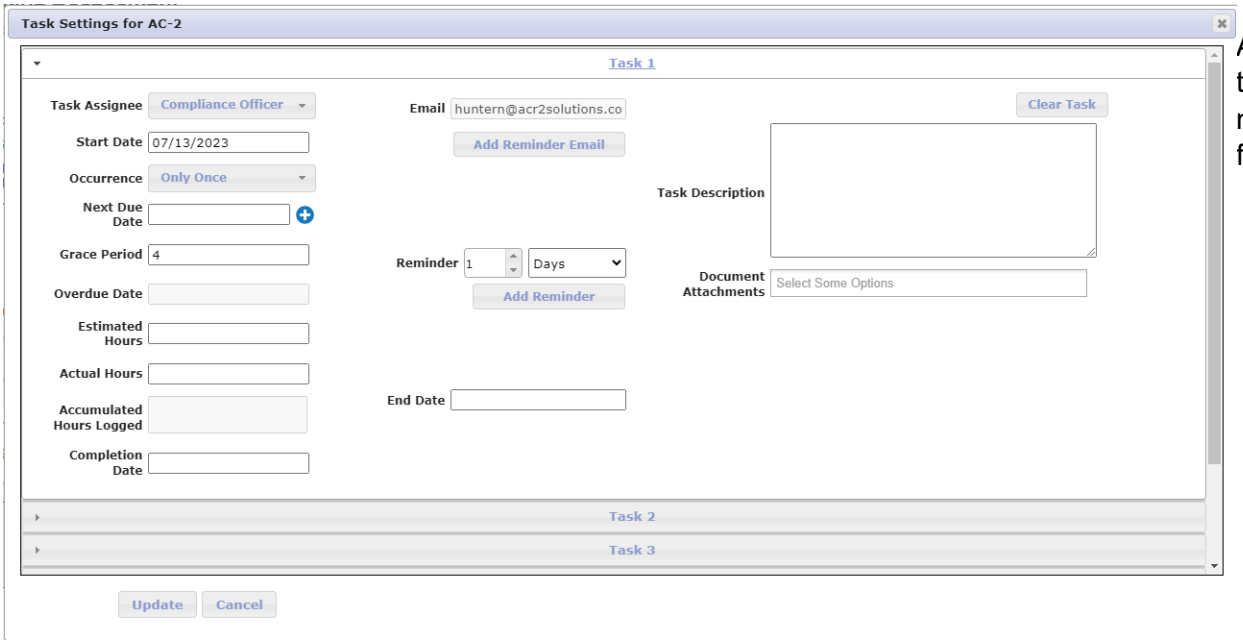
Screen shot of the ACRMS data input page



Question RA-5(5): VULNERABILITY SCANNING

Answer RA-5(5): ☐ Yes ☐ Yes/Alt ☐ No ☐ NA ☒ Partial
Policy File RA-5(5): CUI 3.11.2 RA5 5(5) MoYr

Screen shot of the ARMS task edit page



Access to the network for <quarterly> vulnerability scanning shall be authorized by the <Compliance Officer> and managed by the <IT Manager>. File signed and dated report in Document Management Center (DMC).

Report Example: Vulnerability Scanning Authorization

Access to the network for vulnerability scanning shall be authorized by Bobby Lee and managed by Tommy Lee. Typically, this will be an outside vendor who has been preapproved.

Filename: RA-5(5) Vulnerability Scanning Authorization 09022023

Report Date: 09/02/2023_____

Report Author: Tommy Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Tommy Lee _____

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00		2.00		4.00	

Estimated hours: 4

Appendix D

Quantity	Part #	Product Name	MSRP Price/Disc	TOTAL
0	CUI- Startup - 1 Site 1to50- 1 Month	ACRMS DFARS 252.204-7012 Initial Compliance package - Video Boot Camp augmented Policy package, SSP creation, POAM, implementation and maintenance Task Management setup and scheduling - End with DOD Assessment score- 1 month license - requires NDA. Credit card or check.	$ 999.50	$ -
0	ACRMS MEP/APEX SSP Support	Discounted Video Boot Camp price for clients with a MEP or APEX Accelerator support contract. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/Apex participation in SSP creation.	30%	$ -
1	ACRMS MEP/APEX SSP Support, Pilot study participation	Discounted price for clients with MEP or Apex Accelerator support contract and full MEP/APEX participation in 2024 ACRMS pilot study. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/APEX participation in SSP creation.	50%	$ 499.75
0	ACRMS-CUI-Ongoing Support-1to50-1month	ACRMS subcontractor version: ACRMS Ongoing Policy, SSP & POAM Updating, Task Management System, updates and Technical Support - month by month license - credit card only.	$ 99.50	$ -
0	ACRMS MEP/APEX monthly monitoring Support	Discounted price for clients with MEP or APEX Accelerator support contract. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/APEX participation in monthly monitoring and quarterly meetings.	30%	$ -
6	ACRMS MEP/APEX monthly monitoring Support	Discounted price for clients with MEP or Apex Accelerator support contract and full MEP/APEX participation in 2024 ACRMS pilot study. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/APEX participation in monthly monitoring and quarterly meetings,	50%	$ 298.50
0	ACRMS-CUI-Quarterly Review-1to50-1month	ACRMS Month by Month data analysis, Quarterly Policy and Performance Overview Online Review Meeting - quarterly license - one required for initial SSP or updated account, recommended every 90 days - credit card only.	$ 180.00	$ -
0	ACRMS MEP/APEX quarterly review Support	Discounted price for clients with MEP or APEX Accelerator support contract. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/APEX participation in monthly monitoring and quarterly meetings,	30%	$ -
0	ACRMS MEP/APEX quarterly review Support	Discounted price for clients with MEP or APEX Accelerator support contract and full MEP/APEX participation in 2024 ACRMS pilot study. Requires NDA confirmation, MEP/APEX ACRMS monitoring software and training, MEP/APEX participation in monthly monitoring and quarterly meetings,	50%	$ -
5	CUI SWAT-1yr	Basic CUI Security Awareness online, on-demand, Training in local policies, Testing and Exam for all users - On Demand - 1 Year License - per trainee per year - credit card preferred.	$ 25.00	$ 125.00
0	Consulting	Consulting - per hour - credit card or check	$ 180.00	$ -