



Artifacts Request List

NOTE: All evidence must be in final form and not draft. Unacceptable forms of evidence include but are not limited to working papers, drafts, and unofficial or unapproved policies. Acceptable file formats include but are not limited to .pdf, .xlsx, .png and .jpg. **There should be no open POA&Ms related to implementation of the security requirements.**

Please use the CMMC Level 2 identifiers to identify your artifacts, screenshots, policies and documents. **Ex. AC.L2-3.1.1[a].png, ACME SSP v1.0-CA.L2-3.12.3[a].pdf**

Security System Plans (SSP) file names shall be **less than 45 characters including the file extension**. Additionally, they should reflect your implementation of all 320 Level 2 security requirements. For example if you are annotating your SSP with the requirement identification number **IAW 32 CFR 174.14c** the format is **AC.L2-3.1.1**

If specific evidence is not requested, then be prepared to demonstrate via live screenshare.

Governance and Program Management
• System Security Plan (SSP) • POA&M (Plan of Action & Milestones) • Roles & Responsibilities Matrix • Security policies for each of the 14 control families • Acceptable Use Policy • Training policy and schedule • Risk Management Strategy or Risk Assessment documentation • Asset inventory (hardware, software, cloud services) • Information security continuous monitoring strategy • Incident Response Plan (IRP) and test results • Change management policy & logs • Configuration Management Plan • Data classification guidance and CUI handling procedures • Supplier Risk Management documentation (if applicable)



Please provide evidence of implementation for the following:

Assessment Objective	Description
Access Control (AC)	
Core Evidence	• Access control policy • User account management procedures • Access request/approval forms • Multi-factor authentication (MFA) configurations • Role-based access control matrix • Session timeout settings • System and file permission screenshots/logs • Privileged access procedures and logs • Shared account restrictions & justifications (if any)
3.1.3[c]	designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
3.1.10[c]	Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.
3.1.20[c]	connections to external systems are verified.
3.1.20[d]	the use of external systems is verified.
3.1.22[c]	a review process is in place prior to posting of any content to publicly accessible systems.
3.1.22[d]	content on publicly accessible systems is reviewed to ensure that it does not include CUI.
3.1.22[e]	mechanisms are in place to remove and address improper posting of CUI.
Awareness and Training (AT)	
Core Evidence	• Security awareness training content • Records of training completion • Role-based training for privileged users • Insider threat training (if developed)
3.2.1[c]	managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.

PUBLIC

Public Release Authorized

3.2.1[d]	managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.
3.2.2[b]	information security-related duties, roles, and responsibilities are assigned to designated personnel.
3.2.2[c]	personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.
3.2.3[b]	security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.
Audit and Accountability (AU)	
Core Evidence	• Audit & logging policy • List of systems generating logs • Log retention settings/screenshots • Log review procedures and schedules • Sample audit logs • Log aggregation or SIEM evidence (if in use)
3.3.3[b]	event types being logged are reviewed in accordance with the defined review process.
3.3.3[c]	event types being logged are updated based on the review.
3.3.4[c]	identified personnel or roles are alerted in the event of an audit logging process failure.
3.3.5[b]	defined audit record review, analysis, and reporting processes are correlated.
Configuration Management (CM)	
Core Evidence	• Baseline configurations (gold images, secure baselines) • Configuration management policy • Change request forms and change control board logs • Automated tools or scripts enforcing configuration (e.g., GPOs) • Evidence of system hardening • Mobile device management (MDM) configuration (if applicable)
3.4.1[b]	the baseline configuration includes hardware, software, firmware, and documentation.
3.4.1[c]	the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.
3.4.1[e]	the system inventory includes hardware, software, firmware, and documentation.
3.4.1[f]	the inventory is maintained (reviewed and updated) throughout the system development life cycle.



3.4.2[b]	security configuration settings for information technology products employed in the system are enforced.
3.4.3[a];[b];[c];[d]	Track, review, approve or disapprove, and log changes to organizational systems.
3.4.4	Determine if the security impact of changes to the system is analyzed prior to implementation.
3.4.5[c]	physical access restrictions associated with changes to the system are approved.
3.4.5[g]	logical access restrictions associated with changes to the system are approved.
3.4.5[h]	logical access restrictions associated with changes to the system are enforced.
Identification and Authentication (IA)	
Core Evidence	• Authentication policy (password, MFA) • Screenshots of user login settings • Evidence of unique user IDs • Device authentication process • Credential protection mechanisms
Incident Response (IR)	
Core Evidence	• Incident Response Plan (IRP) • Incident response roles/responsibilities • Record of IR test or tabletop exercise • Sample incident logs (real or redacted) • Communication plan during incidents • Reporting procedure to DoD
Maintenance (MA)	
Core Evidence	• Maintenance policy • Logs of system maintenance (internal and external) • Remote maintenance approval and monitoring procedures • Maintenance tool controls • Equipment sanitization/disposal procedures
3.7.1	system maintenance is performed
3.7.2[a]	tools used to conduct system maintenance are controlled.
3.7.2[b]	techniques used to conduct system maintenance are controlled.



3.7.2[c]	mechanisms used to conduct system maintenance are controlled.
3.7.3	Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.
3.7.4	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.
Media Protection (MP)	
Core Evidence	• Media protection policy • Removable media use restrictions • Media sanitization procedures and logs • Evidence of encrypted media (if used) • CUI marking on media (if applicable)
3.8.2	Determine if access to CUI on system media is limited to authorized users.
3.8.5[b]	accountability for media containing CUI is maintained during transport outside of controlled areas.
3.8.6	Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.
3.8.7	Determine if the use of removable media on system components is controlled.
3.8.8	Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.
3.8.9	Determine if the confidentiality of backup CUI is protected at storage locations.

PUBLIC

Public Release Authorized



Personnel Security (PS)	
Core Evidence	• Background check procedures • Non-disclosure agreements (NDAs) • Termination checklist • Offboarding process documentation • Access revocation logs
3.9.1	Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.
3.9.2[b]	system access and credentials are terminated consistent with personnel actions such as termination or transfer.
3.9.2[c]	the system is protected during and after personnel transfer actions.
Physical Protection (PE)	
Core Evidence	• Facility security plan • Visitor access logs • Badge/access control system evidence • Physical asset inventory • Monitoring camera system logs or configurations (if applicable)
3.10.1[a]	authorized individuals allowed physical access are identified.
3.10.4	Determine if audit logs of physical access are maintained.
3.10.6[b]	safeguarding measures for CUI are enforced for alternate work sites.
Risk Assessment (RA)	
Core Evidence	• Risk assessment report • Risk register • Threat and vulnerability analysis • Remediation plan for identified risks
3.11.1[b]	risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.
3.11.3[a]	vulnerabilities are identified.
3.11.3[b]	vulnerabilities are remediated in accordance with risk assessments.
Security Assessment (CA)	

PUBLIC

Public Release Authorized



Core Evidence	• Security control assessments (internal or third-party) • Continuous monitoring documentation • Policy for security reviews • Tools or methods used to validate control effectiveness • Ongoing compliance tracking reports
3.12.1[b]	security controls are assessed with the defined frequency to determine if the controls are effective in their application.
3.12.2[a];[b];[c]	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational system
3.12.3	Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

PUBLIC

Public Release Authorized

System and Communications Protection (SC)	
Core Evidence	• Network diagrams (logical and physical) • Data flow diagrams showing CUI movement • Encryption configurations and certificates • Firewall and network ACL rules • Secure communications configurations (VPN, TLS, etc.) • Port/protocol/service restriction evidence • DNS security configurations • Isolation of CUI systems (VLANs, segmentation)
3.13.14[a]	use of Voice over Internet Protocol (VoIP) technologies is controlled.
3.13.14[b]	use of Voice over Internet Protocol (VoIP) technologies is monitored.
System and Information Integrity (SI)	
Core Evidence	• Antivirus/EDR deployment and monitoring evidence • Patch management policy • Vulnerability scan results and remediation logs • Alert/notification settings • System monitoring procedures
3.14.7[b]	unauthorized use of the system is identified.