2026

CMMC Level 1 Assessment Scope

(Main Reference: DoD-CIO-00005 (ZRIN 0790-ZA21) Version 2.13 | September 2024 (Latest version)

AMANDA PACE

INTELLICOMM GROUP INC | Palm Coast FL

Table of Contents

What to Include

In Scope Assets

All Assets that process, store, or transmit Federal contract Information (FCI)[1]

Out of Scope Assets

Assets that do NOT process, store, or transmit FCI. Do not include in assessment.[2]

Specialized Assets

Assets that can process, store, or transmit FCI but are unable to be fully secured. These are not part of the Level 1 assessment scope.[3]

Examples:

Internet of Things (IoT) devices and Industrial Internet of Things (IIoT) devices : may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors[4]

Operational Technology (OT): includes industrial control systems, building management systems, fire control systems, and physical access control mechanisms.[5]

Government Furnished Equipment (GFE): includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification.[6]

Restricted Information Systems: means systems [and associated Information Technology (IT) components comprising the system] that are configured based entirely on government security requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).

Test Equipment: means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables.

---

[1] 32 CFR § 170.19(b)
[2] 32 CFR § 170.19(b)(2)
[3] 32 CFR § 170.19(b)(2)(ii)
[4] iot.ieee.org/definition; National Institute of Standards and Technology (NIST) 800-183].
[5] [Source: NIST SP 800-160v2 Rev 1] NOTE: Operational Technology (OT) specifically includes Supervisory Control and Data Acquisition (SCADA); this is a rapidly evolving field. [Source: NIST SP 800-82r3]
[6] 48 CFR § 45.101

Additional Guidance on Level 1

To appropriately scope a Level 1 self-assessment you should consider the people, technology, facilities, and external service providers within its environment that process, store, or transmit FCI. [7]

• People – May include, but are not limited to, employees, contractors, vendors, and external service provider personnel.

• Technology – May include, but are not limited to, servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems.

• Facilities – May include, but are not limited to, physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms.

• External Service Provider (ESP) –means external people, technology, or facilities that you utilize for provision and management of comprehensive IT and/or cybersecurity services. [8]

When is a new assessment required:

A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions.

When your annual affirmation is acceptable:

Operational changes within a CMMC Assessment Scope, such as adding or subtracting resources within the existing assessment boundary that follow the existing SSP[9]

[7] 32 CFR § 170.19(b)(3)
[8] 32 CFR § 170.4
[9] It is recommended that you develop a SSP as a best practice at Level 1. However, it is not required in order to conduct a Level 1 self-assessment.

Assessment

The guidance specified in NIST SP 800-171A focuses on Controlled Unclassified Information (CUI). Since Level 1 focuses on safeguarding FCI, the applicable self-assessment objectives for Level 1 are modified to address FCI rather than CUI as set forth in 32 CFR § 170.15(c)(1)(i). Where CUI is noted in a NIST SP 800-171A assessment objective, [FCI] has been substituted in the Level 1 objective description. Level 1 security requirement descriptions align with FAR Clause 52.204-21.

Documents

For some security requirements, review of documentation may assist an entity in determining if the assessment objectives have been met. Interviews with staff may help identify relevant documents. Documents need to be in their final forms; drafts of policies or documentation are not eligible to be used as evidence because they are not yet official and still subject to change.[10] Common types of documents that may be used as evidence include:

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive.

Assessment Findings

The self-assessment of a CMMC requirement results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE[11]

To demonstrate Level 1 compliance, you will need a finding of MET or NOT APPLICABLE on all Level 1 security requirements.

- MET: All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include working papers, drafts, and unofficial or unapproved policies. For each security requirement marked MET, it is best practice to record statements that indicate the response conforms to all objectives and document the appropriate evidence to support the response.
    - o Enduring Exceptions when described, along with any mitigations, in the system security plan shall be assessed as MET.

[10] 32 CFR § 170.24,
[11] 32 CFR § 170.24.

o Temporary deficiencies that are appropriately addressed in operational plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) shall be assessed as MET.

• NOT MET: One or more objectives of the security requirement is not satisfied. For each security requirement marked NOT MET, it is best practice to record statements that explain why and document the appropriate evidence showing that does not conform fully to all of the objectives. One NOT MET Assessment Objective results in a failure of the entire security requirement. A security requirement can be applicable even when assessment objectives included in the security requirement are scored N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET.

• NOT APPLICABLE (N/A): A security requirement and/or objective do not apply at the time of the assessment. For each security requirement marked N/A, it is best practice to record a statement that explains why the requirement does not apply. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET. Each assessment objective in NIST SP 800-171A must yield a finding of MET or NOT APPLICABLE in order for the overall security requirement to be scored as MET.

For example, SC.L1-b.1.xi might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope.

Satisfaction of security requirements may be accomplished by other parts of the enterprise or an External Service Provider (ESP)[12]. A security requirement is considered MET if adequate evidence is provided that the enterprise or ESP implements the requirement objectives. An ESP may be external people, technology, or facilities that is used, including cloud service providers, managed service providers, managed security service providers, or cybersecurity-as-a-service providers.

[12] 32 CFR § 170.4

Assessment Items

Access Control

AC.L1 – B.1.I – Authorized Access Control [FCI Data]

Identify users, processes, and devices that are allowed to use company computers and can log on to the company network.[13]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Example 1

Your company maintains a list of all personnel authorized to use company information systems [a]. This list is used to support identification and authentication activities conducted by IT when authorizing access to systems [a,d].

Example 2

A coworker wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will prevent network access by unauthorized systems and devices [c]. You help the coworker submit a ticket that asks for the printer to be granted access to the network, and appropriate leadership approves the device [f].

AC.L1-B1.II – Transaction & Function control [FCI Data]

Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[13] NIST SP 800-171 Rev. 2, p.10, FAR Clause 52.204-21 b.1.i, NIST SP 800-171 Rev. 2 3.1.1

[b] system access is limited to the defined types of transactions and functions for authorized users.[14]

Example

You supervise the team that manages DoD contracts for your company. Members of your team need to access the contract information to perform their work properly. Because some of that data contains FCI, you work with IT to set up your group's systems so that users can be assigned access based on their specific roles [a]. Each role limits whether an employee has read-access or create/read/delete/update -access [b]. Implementing this access control restricts access to FCI information unless specifically authorized.[15]

AC.L1-B.1.III – EXTERNAL CONNECTIONS [FCI DATA]

Determine if:

[a] connections to external systems are identified;

[b] the use of external systems is identified;

[c] connections to external systems are verified;

[d] the use of external systems is verified;

[e] connections to external systems are controlled/limited; and

[f] the use of external systems is controlled/limited.[16]

Example

Your company has just been awarded a contract which contains FCI. You remind your coworkers of the policy requirement to use their company laptops, not personal laptops or tablets, when working remotely on this contract [b,f]. You also remind everyone to work from the cloud environment that is approved for processing and storing FCI rather than the other collaborative tools that may be used for other projects [b,f].[17]

AC.L1-B.1.IV – CONTROL PUBLIC INFORMATION [FCI DATA]

Determine if:

[a] individuals authorized to post or process information on publicly accessible systems are identified;

---

[14] NIST SP 800-171A
[15] FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev. 2 3.1.2
[16] NIST SP 800-171A
[17] FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev. 2 3.1.20

[b] procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified;

[c] a review process is in place prior to posting of any content to publicly accessible systems;

[d] content on publicly accessible systems is reviewed to ensure that it does not include [FCI]; and

[e] mechanisms are in place to remove and address improper posting of [FCI].[18]

Example

Your company decides to start issuing press releases about its projects in an effort to reach more potential customers. Your company receives FCI from the government as part of its DoD contract. Because you recognize the need to manage controlled information, including FCI, you meet with the employees who write the releases and post information to establish a review process [c]. It is decided that you will review press releases for FCI before posting it on the company website [a,d]. Only certain employees will be authorized to post to the website [a].[19]

[18] NIST SP 800-171A

[19] FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 Rev. 2 3.1.22

Identification and Authentication (IA)

IA.L1-B.1.V – IDENTIFICATION [FCI DATA]

Determine if:

[a] system users are identified;

[b] processes acting on behalf of users are identified; and

[c] devices accessing the system are identified.[20]

Example You want to make sure that all employees working on a project can access important information about it. Because this is work for the DoD and contains FCI, you also need to prevent employees who are not working on that project from being able to access the information. You assign each employee a unique user ID, which they use to log on to the system [a].[21]

IA.L1-B.1.VI – AUTHENTICATION [FCI DATA]

Determine if:

[a] the identity of each user is authenticated or verified as a prerequisite to system access;

[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and

[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.[22]

Example 1

You are in charge of purchasing laptops that will store FCI. You know that some laptops come with a default username and password. You notify IT that all default passwords should be reset prior to laptop use [a]. You ask IT to explain the importance of resetting default passwords and convey how easily they are discovered using internet searches during next week's cybersecurity awareness training.

Example 2

Your company decides to use cloud services for email and other capabilities that will transmit FCI. Upon reviewing this requirement, you realize every user or device that connects to the cloud service must be authenticated. As a result, you work with your cloud service provider to ensure that only properly authenticated users and devices are allowed to connect to the system [a,c].[23]

---

[20] NIST SP 800-171A
[21] FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev. 2 3.5.1
[22] NIST SP 800-171A
[23] FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev. 2 3.5.2

Media Protection (MP)

MP.L1-B.1.VII – MEDIA DISPOSAL [FCI DATA]

Determine if:

[a] system media containing [FCI] is sanitized or destroyed before disposal; and

[b] system media containing [FCI] is sanitized before it is released for reuse.[24]

Example

As you pack for an office move, you find some old CDs in a file cabinet. You determine that one has FCI from a project your company did for the DoD. You shred the CD rather than simply throwing it in the trash [a].[25]

[24] NIST SP 800-171A

[25] FAR Clause 52.204-21 b.1.vii • NIST SP 800-171 Rev. 2 3.8.3

Physical Protection (PE)

PE.L1-B.1.VIII – LIMIT PHYSICAL ACCESS [FCI DATA]

Determine if:

[a] authorized individuals allowed physical access are identified;

[b] physical access to organizational systems is limited to authorized individuals;

[c] physical access to equipment is limited to authorized individuals; and

[d] physical access to operating environments is limited to authorized individuals.[26]

Example

You manage a DoD project that stores FCI on computers used only by project team members [b,c]. You work with the facilities manager to put locks on the doors to the areas where the computers are stored and used [b,c,d]. Project team members are the only individuals issued with keys to the space. This restricts access to only those employees who work on the DoD project and require access.[27]

PE.L1-B.1.IX – MANAGE VISITORS & PHYSICAL ACCESS [FCI DATA]

Determine if:

[a] visitors are escorted;

[b] visitor activity is monitored;

[c] audit logs of physical access are maintained;

[d] physical access devices are identified;

[e] physical access devices are controlled; and

[f] physical access devices are managed.[28]

Example 1

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office where FCI is stored. You know this person well and trust them, but are not sure why they are in the building. You stop to talk, and the person explains that they are meeting a coworker for lunch, but cannot remember where the lunchroom is. You walk the person back to the reception area to get a visitor badge and wait until someone can escort them to the lunchroom [a]. You

[26] NIST SP 800-171A
[27] FAR Clause 52.204-21 b.1.viii • NIST SP 800-171 Rev. 2 3.10.1
[28] NIST SP 800-171A

report this incident, and the company decides to install a badge reader at the main door so visitors cannot enter without an escort [a].

Example 2

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company has just signed a contract with the DoD in which your company will receive FCI and you now need to document who enters and leaves your facility. You work with the reception staff to ensure that all non-employees sign in at the reception area and sign out when they leave [c]. You retain those paper sign-in sheets in a locked filing cabinet for one year. Employees receive badges or key cards that enable tracking and logging access to company facilities.

Example 3

You are a facility manager. A team member retired today and returns their company keys to you. The project on which they were working requires access to areas that contain equipment with FCI. You receive the keys, check your electronic records against the serial numbers on the keys to ensure all have been returned, and mark each key returned [f].[29]

[29] FAR Clause 52.204-21 b.1.ix • NIST SP 800-171 Rev. 2 3.10.3 • NIST SP 800-171 Rev. 2 3.10.4 • NIST SP 800-171 Rev. 2 3.10.5

System and Communications Protection (SC)

SC.L1-B.1.X – BOUNDARY PROTECTION [FCI DATA]

Determine if:

[a] the external system boundary is defined;

[b] key internal system boundaries are defined;

[c] communications are monitored at the external system boundary;

[d] communications are monitored at key internal boundaries;

[e] communications are controlled at the external system boundary;

[f] communications are controlled at key internal boundaries;

[g] communications are protected at the external system boundary;

[h] and communications are protected at key internal boundaries.[30]

Example

You are setting up the new network with an FCI enclave. You start by sketching out a simple diagram that identifies the external boundary of your network and any internal boundaries that are needed [a,b]. The first piece of equipment you install is the firewall, a device to separate your internal network from the internet. The firewall also has a feature that allows you to block access to potentially malicious websites, and you configure that service as well [a,c,e,g]. Some of your coworkers complain that they cannot get to certain websites [c,e,g]. You explain that the new network blocks websites that are known for spreading malware. The firewall sends you a daily digest of blocked activity so that you can monitor the system for attack trends [c,d].[31]

SC.L1-B.1.XI – PUBLIC-ACCESS SYSTEM SEPARATION [FCI DATA]

Determine if:

[a] publicly accessible system components are identified; and

[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.[32]

Example

[30] NIST SP 800-171A]
[31] FAR Clause 52.204-21 b.1.x • NIST SP 800-171 Rev. 2 3.13.1
[32] NIST SP 800-171A

The head of recruiting at your firm wants to launch a website to post job openings and allow the public to download an application form [a]. After some discussion, your team realizes it needs to use a firewall to create a perimeter network to do this because your network contains FCI [b]. You host the server separately from the company's internal network where FCI is stored and make sure the network on which it resides is isolated with the proper firewall rules [b].[33]

[33] FAR Clause 52.204-21 b.1.xi • NIST SP 800-171 Rev. 2 3.13.5

System and Information Integrity (SI)

SI.L1-B.1.XII – FLAW REMEDIATION [FCI DATA]

Determine if:

[a] the time within which to identify system flaws is specified;

[b] system flaws are identified within the specified time frame;

[c] the time within which to report system flaws is specified;

[d] system flaws are reported within the specified time frame;

[e] the time within which to correct system flaws is specified;

[f] and system flaws are corrected within the specified time frame.[34]

Example

You know that software vendors typically release patches, service packs, hot fixes, etc. and want to make sure your software that processes FCI is up to date. You develop a policy that requires checking vendor websites for flaw notifications every week [a]. The policy further requires that those flaws be assessed for severity and patched on end-user computers once each week and servers once each month [c,e]. Consistent with that policy, you configure the system to check for updates weekly or daily depending on the criticality of the software [b,e]. Your team reviews available updates and implements the applicable ones according to the defined schedule [f].[35]

SI.L1-B.1.XIII – MALICIOUS CODE PROTECTION [FCI DATA]

Determine if:

[a] designated locations for malicious code protection are identified; and

[b] protection from malicious code at designated locations is provided.[36]

Example

Your company's IT team is buying new computers and wants to protect your company's information from viruses and spyware. The computers will be used to process, store, and transmit FCI. They research anti-malware products, select an appropriate solution, and deploy antivirus software on all hosts for which satisfactory antivirus software is available [a,b].[37]

---

[34] NIST SP 800-171A
[35] FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 Rev. 2 3.14.1
[36] NIST SP 800-171A
[37] FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 Rev. 2 3.14.2

SI.L1-B.1.XIV – UPDATE MALICIOUS CODE PROTECTION [FCI DATA]

Determine if: [a] malicious code protection mechanisms are updated when new releases are available.[38]

Example

You have installed anti-malware software to protect a computer that stores FCI from malicious code. Knowing that malware evolves rapidly, you configure the software to automatically check for malware definition updates every day and update as needed [a].[39]

SI.L1-B.1.XV – SYSTEM & FILE SCANNING [FCI DATA]

Determine if:

[a] the frequency for malicious code scans is defined;

[b] malicious code scans are performed with the defined frequency; and

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.[40]

Example

Your company transmits FCI over email. You work with your company's email provider to enable enhanced protections that will scan all attachments to identify and quarantine those that may be harmful prior to a user opening them [c]. In addition, you configure antivirus software on each computer to scan for malicious code every day [a,b]. The software also scans files that are downloaded or copied from removable media such as USB drives. It quarantines any suspicious files and notifies the security team [c].[41]

[38] NIST SP 800-171A
[39] FAR Clause 52.204-21 b.1.xiv • NIST SP 800-171 Rev. 2 3.14.4
[40] NIST SP 800-171A
[41] FAR Clause 52.204-21 b.1.xv • NIST SP 800-171 Rev. 2 3.14.5

Attesting your Score on SPRS

Overview

This checklist walks your organization through **CMMC Level 2 self-attestation**, including required registrations, role setup, documentation, and submission to the DoD.

Company Registration & System Access

Register in SAM.gov

Purpose: Required to do business with the U.S. Government.

Actions:

- Register or verify your entity at **SAM.gov**
- Obtain a valid **CAGE Code**
- Confirm registration is **Active**

PIEE Registration & Role Assignment

Register in PIEE (Procurement Integrated Enterprise Environment)

Purpose: Provides access to systems required for CMMC compliance and SPRS submission.

Actions:

- Add Your CAGE Code to the PIEE Vendor Group Structure by Contacting the PIEE Help Desk by phone or email: 1-866-618-5988
- A company representative must request your CAGE Code to be added to a Vendor Group in the Procurement Integrated Enterprise Environment (PIEE).
- Provide your CAGE Code and desired Group Name. If you don't specify a Group Name, one will be assigned based on your CAGE Code or company name.
- Go to PIEE and click **Register**
- Select organization type:
    - **Vendor** OR
    - **Contractor** (either is acceptable)

Assign Contractor Administrator Manager (CAM) *(Done During Registration)*

Important:

The **CAM is designated during the PIEE registration process**

Requirements:

- Designate **one primary individual**
- This person should:
    - Be responsible for IT or cybersecurity
    - Serve as the main compliance point of contact

Responsibilities:

- Manage PIEE account and user roles
- Oversee SPRS submissions
- Maintain compliance documentation

Complete PIEE Registration

- Finish all required fields and organization setup
- Confirm account activation

Additional Role Configuration *(Done After Registration)*

Assign Cyber Vendor User Role

Purpose: Enables access to SPRS and cybersecurity modules.

Actions:

- Assign **Cyber Vendor User role** within PIEE
- Recommended: assign to the **same person as CAM**

Verify SPRS Access

Purpose: SPRS is where CMMC self-assessment scores are submitted.

Actions:

- Log into PIEE dashboard
- Confirm **SPRS (Supplier Performance Risk System)** appears
- If not:

- Log out and back in
- Verify correct role assignment

CMMC Level 1 – Security Self-Assessment

Complete DoD Self-Assessment

Purpose: Evaluate compliance with required security controls.

Actions:

- Use: **DoD Self-Assessment & SPRS Scoring Methodology (latest version available at CMMC | Intellicomm Group Inc)**
- Answer all applicable controls
- Calculate your **SPRS Score**

Note:
Level 1 focuses on **basic safeguarding of Federal Contract Information (FCI)**.

Required Security Documentation

Create System Security Plan (SSP)

Purpose: Documents your security controls and system environment.

Include:

- System scope and boundaries
- Hardware/software inventory
- Security controls in place
- Data handling processes (FCI)
- Access control methods

Create Incident Response Plan (IRP)

Purpose: Defines how your organization handles cybersecurity incidents.

Include:

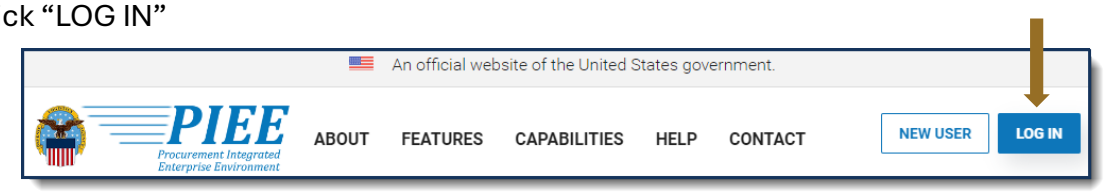
- Incident definitions
- Roles and responsibilities
- Response procedures
- Reporting requirements
- Key contacts

SPRS Submission & Attestation[42]

1. **PIEE Access:** A "SPRS Cyber Vendor User" role is required to enter CMMC Assessment information. PIEE Access Instructions: https://www.sprs.csd.disa.mil/access.htm

2. SPRS Application and Module Access:
   a. PIEE landing page: https://piee.eb.mil

   b. Click "LOG IN"



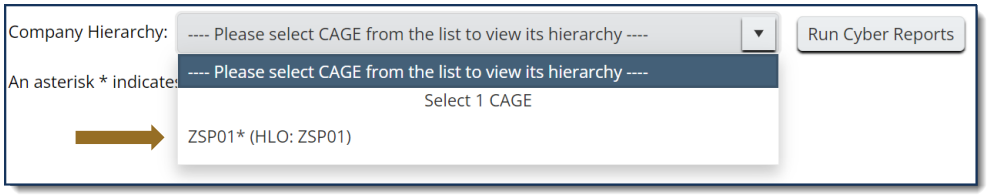
Screenshot Dtd 09 JAN 2024

   c. Select **SPRS**:

   d. Select **Cyber Reports**:

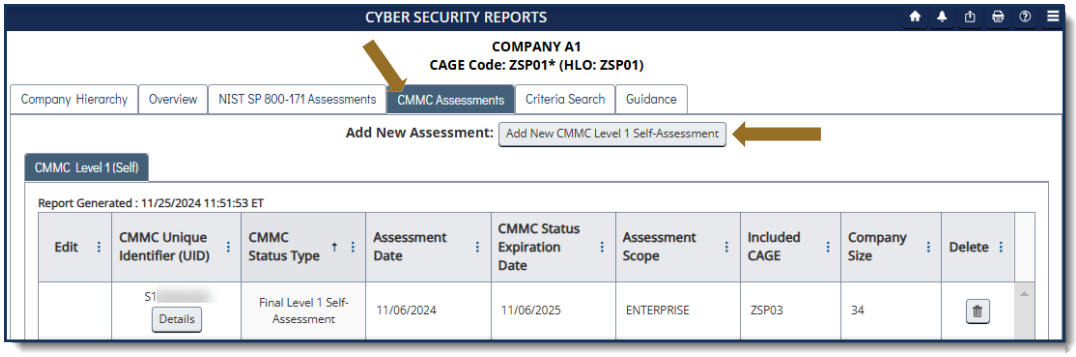
3. **Cyber Reports Module:** Select the desired Hierarchy, identified by the HLO, from the drop down.

[42] CMMC LEVEL 1 SELF-ASSESSMENT QUICK ENTRY GUIDE VERSION 4.0



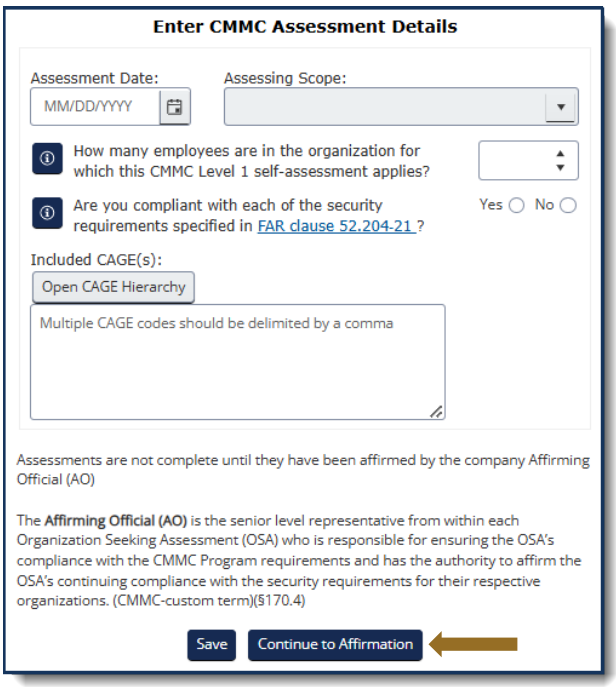
NOTE: An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit/delete)

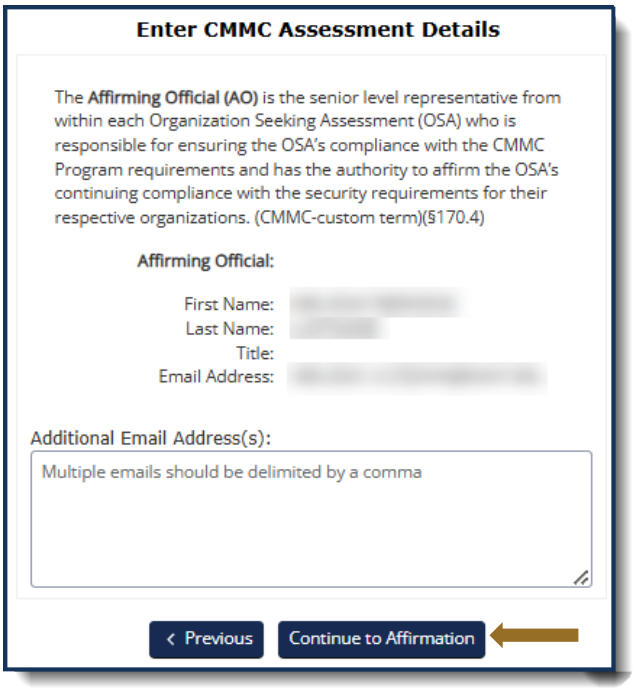
3.1 Add New Assessment: Within the CMMC Assessments tab, select "Add New Level 1 CMMC Self-Assessment".



3.2 Enter Assessment Details: Enter assessment data and select "Continue to Affirmation".

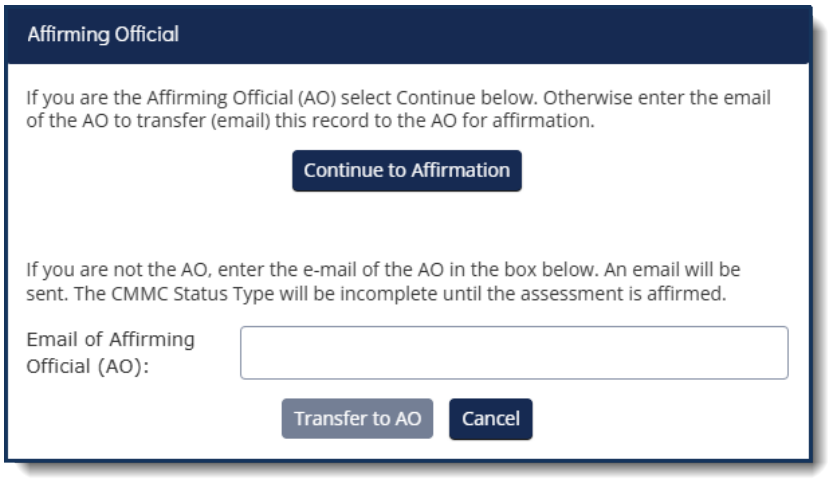
NOTE: Compliance with the security requirements specified in FAR clause 52.204–21 is required to achieve a "Final Level 1 Self-Assessment".



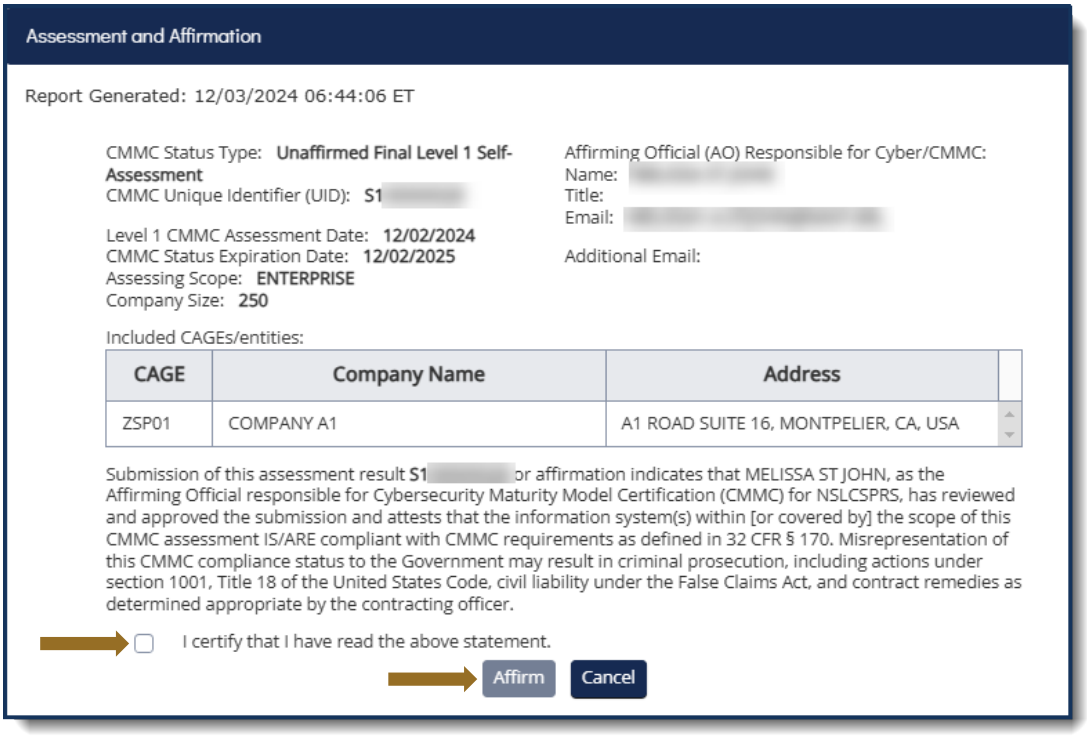


NOTE: CAGE Hierarchy is imported from the System for Award Management (SAM

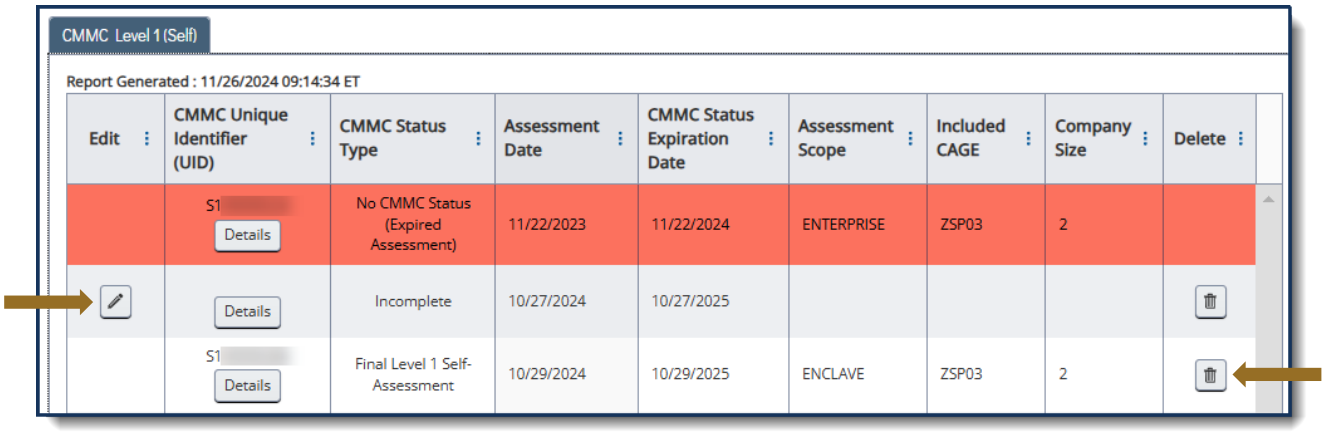
3.3 Transfer to Affirming Official (AO): If the user entering the assessment is not the AO, the assessment can be forwarded via email, to the AO by entering their email and selecting "Transfer to AO".



3.4 Affirm the Assessment: Review the assessment details, certify review of the affirmation statement, and select "Affirm".



3.5 Assessment Edit/Delete: A Cyber Vendor User may edit or delete certain CMMC Status Types.



NOTE: A "Final Level 1 Self-Assessment" will automatically become "No CMMC Status (Expired Assessment)" after 1 year.

NOTE: "Final Level 1 Self-Assessment" is the only CMMC Status Type that will be visible to Government Personnel.

Ongoing Compliance

Maintain Documentation

- Keep SSP, IRP, and assessment records updated
- Store documentation securely

Annual Review

- Review controls at least once per year
- Update documents as needed
- Reassess if systems or contracts change
