ANCHOR SECURITY ARCHITECTURE FOR CMMC 2.0

Simple architecture for CMMC compliance with Anchor desktop platform

Abstract

We provide a brief introduction to the basic requirements of the CMMC 2.0 and how Anchor can be used to reduce the cost and effort to become CMMC certified. To that end, we provide a security architecture that is broad and easy to implement for a variety of organizations. We provide examples of IT infrastructures and how the architecture can fit custom to each. Lastly, we provide a detailed mapping exercise, clearly illustrating the domains and sub-domains that are covered by the Anchor platform independently or with the support of other solutions.

Anchor compliance documents

support@datanchor.io

Table of Contents

Introduction

The **Cybersecurity Maturity Model Certification (CMMC)** is a certification, contractors need before they can perform work for the Department of Defense. All suppliers including small and medium sized businesses must implement CMMC 2.0 level 2 or higher to maintain business within the Department of Defense supply chain. The CMMC framework is built on the NIST 800-171 foundation, which the Defense Industrial Base (DIB) has been attesting to, since 2017 for their contracts.

This document explains the key aspects of the CMMC and how Anchor can be used to reduce the cost and effort to become CMMC certified.

What is different in CMMC 2.0?

- Move from 5 levels to 3 levels of data sensitivity.
    - Level 1 (Foundational) only applies to companies that focus on the protection of Federal Contract Information (FCI).
    - Level 2 (Advanced) is for companies working with Controlled Unclassified Information (CUI).
    - Level 3 (Expert) is focused on reducing the risk from Advanced Persistent Threats (APTs).
- From an absolute Pass/Fail system of the original CMMC, there is a composite, 1, 3, and 5-point scoring system for controls.
- CMMC 2.0 requirements can be in contracts as soon as March 2023
- The Department of Justice offers monetary incentives for whistle-blowers. False attestation to the original NIST controls will lead to penalties, 20% of which is passed on to the whistle-blower.

What Is a System Security Plan?

A security plan simply describes what an organization does in order to be secure. How do you know your organization is secure? Because you do the things in your security plan.

As for CMMC, your **System Security Plan (SSP)** describes how you protect sensitive information from the government such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

From CMMC CA.L2-3.12.4:

“A system security plan (SSP) is a document that outlines how an organization implements its security requirements. An SSP outlines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows.”

Being certified for CMMC means having an auditor review your organization’s SSP to ensure it meets all of the requirements for the CMMC level at which you’re being certified, and verifying that your organization is actually doing everything you claim in your SSP.

What Is a Covered Contractor Information System?

A **Covered Contractor Information System** defines the boundaries of connected network of computers and devices that process sensitive data from the government such as FCI and CUI.

Anything that contains or processes this kind of information is part of the covered contractor information system. Your SSP must thoroughly cover your entire covered contractor information system. Limiting and reducing the scope of devices that can process FCI and CUI reduces the size of your covered contractor information system and therefore simplifies the SSP needed to protect it.

The simpler your SSP, the easier it is to create, implement, and audit. Easier means faster and at a lower cost. The formula to reduce your cost and effort to be CMMC certified is:

1. Limit and reduce the scope of your covered contractor information system.
2. Create a simpler SSP to protect that covered contractor information system.
3. **Save on cost and effort implementing your SSP and getting CMMC certified.**

What Is a Security Architecture?

A **Security Architecture** is the technical design of your covered contractor information system, including what is in it, how it all fits together, and how it enables controls to implement your SSP.

Security Architecture

In this section, we provide the proposed security architecture with the Anchor platform. The architecture is simple and broad; it applies to a variety of business scenarios, covering a wide range of industries with different IT infrastructure, from very elementary to sophisticated and hybrid.

The High-Level Architecture

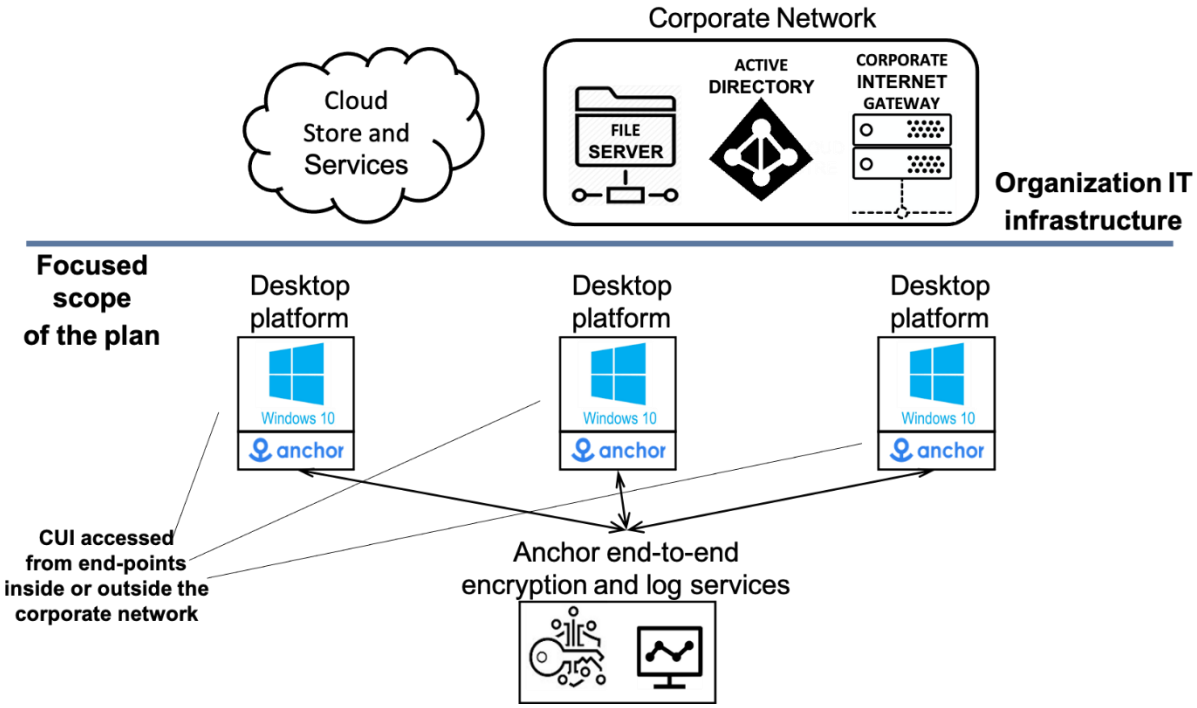

Figure 1: Anchor simplifies CMMC compliance by reducing the system boundary to a narrow set of Anchored files that are accessed and processed at the Anchor-enrolled endpoints (below the blue line). CUI is end-to-end encrypted by Anchor with FIPS-validated cryptography. The compliant architecture is independent of the IT infrastructure (above the blue line). Thus, the mapped domains are covered for a broad set of organizations with various sophistication.

The proposed architecture is illustrated in Figure 1. With Anchor, the "system" is the set of Anchor-enabled devices containing CUI. Anchor simplifies CMMC compliance by reducing the system boundary from a complex network to a narrow set of Anchored files that are end-to-end encrypted by Anchor with FIPS-validated cryptography [CMVP].

At the heart of our architecture lies the fact that Anchored CUI can only be consumed at Anchor-enabled endpoints due to the robust end-to-end encryption system integrated into the desktop platform built by Anchor. The key management, and audit logging services are both provided by the Anchor platform, external to the desktop agent. These services provide the secure access management and audit log creation in coordination with the desktop platform, with components orthogonal to the rest of the organization IT infrastructure (above the blue line in Figure 1), making the implementation of the security plan **simpler, lower cost, and more robust**.

End-point users are managed by Active Directory (local or Azure). The CUI files can be stored on a network drive or a cloud store, but they cannot be decrypted on those drives due to end-to-end encryption. As the CUI is always encrypted at rest, each device containing CUI is treated as a mobile device.

Examples of IT Infrastructures

In this section, we provide a few sample IT architectures with possible use cases associated. As discussed in the last section, end-to-end encryption provided over the Anchor platform supports the security architecture for internal collaboration over a variety of use cases (illustrated in Figure 2).

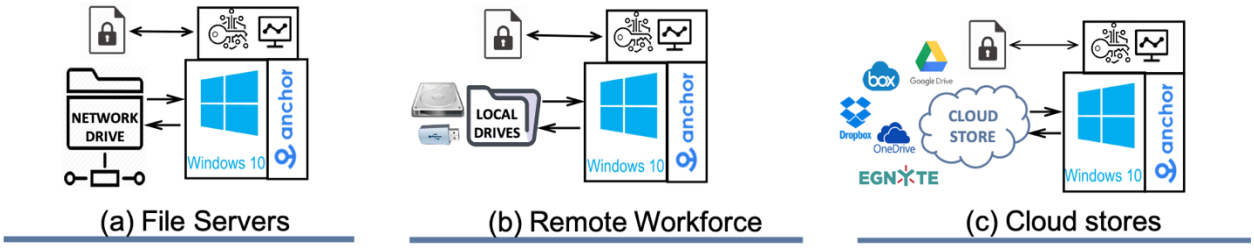

Figure 2: End-to-end encryption across endpoints makes it possible to collaborate on unstructured data over a variety of data stores.

(a) Many organizations keep CUI internally within their network at local file servers (mainly over Windows Server OS). For example, **manufacturing**, **construction**, and **high-tech engineering** organizations, building products and IP for the DoD use a variety of file types and applications, including CAD and Office. Anchor keeps the designs, associated IP, contracts, and calculations encrypted in the file server, while enabling access from the desired applications shown in Figure 3 without a change in the workflow or the application itself. Directories and CUI files are stored on a network drive but cannot be decrypted on that drive due to end-to-end encryption. As the CUI is always encrypted at rest, each device containing CUI is treated as a mobile device.
As a result, CUI is protected automatically as per CMMC, while the organization does not lose any efficiency in processing the data.

Figure 3: Anchor platform has support for a wide variety of applications that encompass CAD and Office. It enables secure and no-friction access and collaboration on the associated files.

(b) With the pandemic, organizations have a considerable amount of its workforce needing to access CUI remotely. In such cases, files are downloaded to the local drives for processing. This is sometimes despite the policies on VPN use, due to the performance issues associated with remote consumption. Such local store and access inflate the attack surface and makes the CUI policies difficult to enforce.

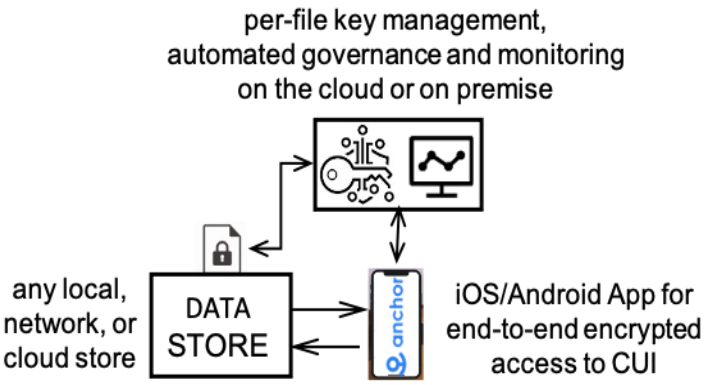

Figure 4: Anchor platform extends its end-to-end encryption to the mobile platforms including iOS and Android. As a result, files can be viewed from smart phones and tablets.

With the Anchor platform, this would not pose a problem. An admin can simply include the local drive as a protected area and make sure that the CUI remains safe, even when accessed remotely by the employees or contractors. Furthermore, Anchor's protection extends to a Mobile App for **iPhone and Android platforms**, as shown in Figure 4. As a result, CUI can be accessed from smart phones and tablets.

(c) Organizations are moving to a hybrid IT infrastructure with cloud applications and data stores involved in everyday processes. Most organizations will have certain processes handled over FedRAMP High government clouds such as Microsoft GCC High. However, it is likely that there will be applications and processes involving CUI on commercial cloud as well. Anchor platform provides the flexibility of protecting data on commercial cloud due to its robust end-to-end encryption integrated.

DFARS 7012 and **ITAR** have additional requirements, such as information must not be exported out of the United States. This creates an obstacle to using commercial cloud storage because commercial clouds store data outside the US and are administrated by people outside the US. However, they carve out an exception when the information end-to-end encrypted with FIPS-validated cryptography. With Anchor end-to-end encryption you can store data on commercial clouds and still be compliant.

CMMC Mapping

Assuming the security architecture described above, we provide a breakdown of the CMMC Level 2 practices by whether and how they can be covered with Anchor. We also provide supplemental text that can be used in your SSP as a template.

Each practice is labeled as one of:

Covered	The Anchor security architecture effectively implements the practice.
Shared Coverage	The Anchor security architecture contributes to implementing the practice, but complete coverage will require additional contribution from the customer.
Customer Responsibility	The customer is responsible for implementing the practice entirely.

Access Control (AC)

AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
Covered	[a] Authorized users are identified by being members of the CUI group in Active Directory. [b] Processes acting on behalf of authorized users are identified by being authorized applications in Anchor. [c] Devices (and other systems) authorized to connect to the system are identified by being devices (e.g., printers) accessible in the CUI Group Policy. [d] System access is limited to authorized users by the CUI Group Policy that restricts logins to members of the GUI group. [e] System access is limited to processes acting on behalf of authorized users by being Anchor authorized applications. [f] System access is limited to authorized devices (including other systems) by the CUI Group Policy.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
Covered	[a] The types of transactions and functions that authorized users are permitted to execute are defined by their Anchor user role. [b] System access is limited to the defined types of transactions and functions for authorized users by Anchor's enforcement of user roles.
AC.1.003	Verify and control/limit connections to and use of external information systems.
Covered	[b] The use of external systems is identified by having Anchor software installed and being logged with a user role that can access CUI. [d] The use of CUI on external systems is verified by Anchor when a CUI file is opened on an external device. [f] The use of CUI on external systems is controlled/limited by Anchor.
Customer Responsibility	[a] Connections to external systems are identified. [c] Connections to external systems are verified. [e] Connections to external systems are controlled/limited.

AC.1.004	Control information posted or processed on publicly accessible information systems.
Customer Responsibility	[a] Individuals authorized to post or process information on publicly accessible systems are identified. [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. [e] Mechanisms are in place to remove and address improper posting of FCI.
AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.
Customer Responsibility	[a] Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category. [b] Privacy and security notices are displayed.
AC.2.006	Limit use of portable storage devices on external systems.
Covered	[a] Any portable storage device can be used to transfer anchored files containing CUI. [b] Portable storage devices may only be used to transfer anchored files containing CUI. They may not contain unanchored CUI files. [c] The files are encrypted at rest. Anchor will only allow CUI files to be opened on internal devices and approved external devices.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.
Customer Responsibility	[a] Privileged accounts are identified. [b] Access to privileged accounts is authorized in accordance with the principle of least privilege. [c] Security functions are identified. [d] Access to security functions is authorized in accordance with the principle of least privilege.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.
Customer Responsibility	[a] Nonsecurity functions are identified. [b] Users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

AC.2.009	Limit unsuccessful logon attempts.
Customer Responsibility	[a] The means of limiting unsuccessful logon attempts is defined. [b] The defined means of limiting unsuccessful logon attempts is implemented.
AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
Customer Responsibility	[a] The period of inactivity after which the system initiates a session lock is defined. [b] Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity. [c] Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.
AC.2.011	Authorize wireless access prior to allowing such connections.
Shared responsibility	General wireless access control is beyond the scope of Anchor responsibility. However, once CUI is anchored and the CUI system boundary is defined by Anchor access rules, there are no wireless access points within the system boundary because we have used Anchor to limit system scope to authorized mobile endpoints.
AC.2.013	Monitor and control remote access sessions.
Shared responsibility	Monitoring of general access to the CUI servers and devices is beyond the scope of Anchor controls. However, once CUI is accessed, that information is logged. Further, if remote access to the anchored devices is eliminated, there is no remote access to the system because we have used Anchor to limit system scope to authorized mobile endpoints which don't provide remote access.
AC.2.015	Route remote access via managed access control points.
Shared responsibility	Routing of remote access is beyond the scope of Anchor controls. However, if remote access to the anchored CUI systems is eliminated, there is no remote access to the system because we have used Anchor to limit system scope to authorized mobile endpoints which don't provide remote access.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.
Covered	[a] CUI must be anchored, and therefore end-to-end encrypted, in order to flow out of the system.

	[b] Files containing CUI are anchored at all times and are therefore end-to-end encrypted at rest. Any file leaving the system is already encrypted. [c] Designated sources and destinations for CUI are identified by having Anchor installed and the user belonging to the CUI group. [d] Authorizations for controlling the flow of CUI are defined by the Anchor User Role. [e] Approved authorizations for controlling the flow of CUI are enforced by Anchor.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
Customer Responsibility	[a] The duties of individuals requiring separation are defined. [b] Responsibilities for duties that require separation are assigned to separate individuals. [c] Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
Customer Responsibility	[a] Privileged functions are defined. [b] Non-privileged users are defined. [c] Non-privileged users are prevented from executing privileged functions. [d] The execution of privileged functions is captured in audit logs.
AC.3.019	Terminate (automatically) user sessions after a defined condition.
Shared Responsibility	Customer should configure the OS to to terminate user sessions after 15 minutes of inactivity. With Anchor, more sophisticated access controls (e.g., attribute or location based) can be added to the rules to revoke access beyond further governance rules.
AC.3.012	Protect wireless access using authentication and encryption.
Shared Responsibility	Setting up the routers with proper authentication and connection encryption is customer responsibility. However, the customer may choose to set up Anchor to limit the system scope to authorized mobile endpoints. As a result, there are no wireless access points within the system boundary.

AC.3.020	Control connection of mobile devices.
Covered	[a] Mobile devices that process, store, or transmit CUI are identified by having Anchor software installed and the user belonging to the CUI group. [b] Mobile device connections to CUI are authorized by Active Directory and Anchor. [c] Mobile device connections to CUI are monitored and logged by Active Directory and Anchor.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
Shared Responsibility	Configuring the remote access session payloads to be encrypted is customer responsibility. However, customer may choose to use Anchor to limit system scope to authorized mobile endpoints which don't provide remote access to satisfy the controls.
AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.
Customer Responsibility	[a] Privileged commands authorized for remote execution are identified. [b] Security-relevant information authorized to be accessed remotely is identified. [c] The execution of the identified privileged commands via remote access is authorized. [d] Access to the identified security-relevant information via remote access is authorized.
AC.3.022	Encrypt CUI on mobile devices and mobile computing platforms.
Covered	[a] Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified by having Anchor software and belong to the CUI group. [b] Anchor encrypts CUI files with Microsoft CNG, a FIPS-validated module. [CVMP]

Asset Management (AM)

AM.3.036	Define procedures for the handling of CUI data.
Customer Responsibility	[a] the organization establishes and maintains one or more processes or procedures for handling CUI data.

Awareness and Training (AT)

AT.2.056	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
Customer Responsibility	[a] Security risks associated with organizational activities involving CUI are identified. [b] Policies, standards, and procedures related to the security of the system are identified. [c] Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities. [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.
AT.2.057	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
Customer Responsibility	[a] Information security-related duties, roles, and responsibilities are defined. [b] Information security-related duties, roles, and responsibilities are assigned to designated personnel. [c] Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.
AT.3.058	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
Customer Responsibility	[a] Potential indicators associated with insider threats are identified. [b] Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Audit and Accountability (AU)

AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Shared Responsibility	[a] Every create/anchor, open, save, access denied, and unAnchor event is logged for every CUI file including user information. Other actions as well as non-CUI interactions on devices should be logged by the customer. [b] Anchor records and maintains these logs for 1 year, and makes them available in the Anchor dashboard.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
Shared Responsibility	[a] Anchor logs are specified as needed for CUI. General system audit logs with high-level file operations and non-CUI are customer responsibility. [b] Every create/anchor, open, save, access denied, and unanchor event is logged for every CUI file including timestamp, IP address, user, process/application, event descriptions, success/failure, and filenames. [c] Anchor generates the audit logs each time an attempt is made to access a CUI file. [d] Anchor generated logs include the defined content. [e] Audit logs are maintained for 1 year. [f] Anchor records and maintains these logs for 1 year, and makes them available in the Anchor dashboard.
AU.2.043	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
Customer Responsibility	[a] Internal system clocks are used to generate time stamps for audit records. [b] An authoritative source with which to compare and synchronize internal system clocks is specified. [c] Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.
AU.2.044	Review audit logs.
Customer Responsibility	[a] The organization defines one or more policies and/or procedures for the event types to look for when information system audit records are reviewed and analyzed. [b] The organization defines one or more policies and/or procedures for the frequency to review and analyze information system audit records for indications of organizationally defined events.

	[c] The organization reviews and analyzes information system audit records for indications of organizationally defined events with the organization-defined frequency.
AU.3.045	Review and update logged events.
Customer Responsibility	[a] A process for determining when to review logged events is defined. [b] Event types being logged are reviewed in accordance with the defined review process. [c] Event types being logged are updated based on the review.
AU.3.046	Alert in the event of an audit logging process failure.
Customer Responsibility	[a] Personnel or roles to be alerted in the event of an audit logging process failure are identified. [b] Types of audit logging process failures for which alert will be generated are defined. [c] Identified personnel or roles are alerted in the event of an audit logging process failure.
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.
Customer Responsibility	[a] The organization defines information system components that generate audit records whose content is to be centrally managed and configured. [b] The organization manages audit information in centralized repositories. [c] The central repositories have the appropriate infrastructure and capacity to meet the organizationally defined logging requirements.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
Customer Responsibility	[a] Audit information is protected from unauthorized access. [b] Audit information is protected from unauthorized modification. [c] Audit information is protected from unauthorized deletion. [d] Audit logging tools are protected from unauthorized access. [e] Audit logging tools are protected from unauthorized modification. [f] Audit logging tools are protected from unauthorized deletion.

AU.3.050	Limit management of audit logging functionality to a subset of privileged users.
Shared Responsibility	[a] Access to Anchor logs is limited to Anchor administrators. Customer is responsible for the management of all other logs. [b] Anchor limits audit logging functionality to Anchor administrators.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
Customer Responsibility	[a] Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined. [b] Defined audit record review, analysis, and reporting processes are correlated.
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.
Customer Responsibility	[a] An audit record reduction capability that supports on-demand analysis is provided. [b] A report generation capability that supports on-demand reporting is provided.

Security Assessment (CA)

CA.2.157	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
Customer Responsibility	[a] A system security plan is developed. [b] The system boundary is described and documented in the system security plan. [c] The system environment of operation is described and documented in the system security plan. [d] The security requirements identified and approved by the designated authority as non-applicable are identified. [e] The method of security requirement implementation is described and documented in the system security plan. [f] The relationship with or connection to other systems is described and documented in the system security plan. [g] The frequency to update the system security plan is defined.

	[h] System security plan is updated with the defined frequency.
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
Customer Responsibility	[a] The frequency of security control assessments is defined. [b] Security controls are assessed with the defined frequency to determine if the controls are effective in their application.

CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
Customer Responsibility	[a] Deficiencies and vulnerabilities to be addressed by the plan of action are identified. [b] A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities. [c] The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Customer Responsibility	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.
Customer Responsibility	[a] The organization reviews internally developed software for risks. [b] For the code that is defined as an area of risk, the organization has documented the security assessment process which may include one or more of the following: manual code review, static analysis, and/or dynamic analysis. [c] The organization has the ability to demonstrate their security assessment process. [d] The security assessment process is integrated with the change management process.

Configuration Management
(CM)

CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
Customer Responsibility	[a] A baseline configuration is established. [b] The baseline configuration includes hardware, software, firmware, and documentation. [c] The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle. [d] A system inventory is established. [e] The system inventory includes hardware, software, firmware, and documentation. [f] The inventory is maintained (reviewed and updated) throughout the system development life cycle.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
Customer Responsibility	[a] Essential system capabilities are defined based on the principle of least functionality. [b] The system is configured to provide only the defined essential capabilities.
CM.2.063	Control and monitor user-installed software.
Customer Responsibility	[a] A policy for controlling the installation of software by users is established. [b] Installation of software by users is controlled based on the established policy. [c] Installation of software by users is monitored.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.
Customer Responsibility	[a] Security configuration settings for information technology products employed in the system are established and included in the baseline configuration. [b] Security configuration settings for information technology products employed in the system are enforced.
CM.2.065	Track, review, approve or disapprove, and log changes to organizational systems.
Customer Responsibility	[a] Changes to the system are tracked. [b] Changes to the system are reviewed.

	[c] Changes to the system are approved or disapproved. [d] Changes to the system are logged.
CM.2.066	Analyze the security impact of changes prior to implementation.
Customer Responsibility	[a] The security impact of changes to the system is analyzed prior to implementation.
CM.3.067	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
Customer Responsibility	[a] Physical access restrictions associated with changes to the system are defined. [b] Physical access restrictions associated with changes to the system are documented. [c] Physical access restrictions associated with changes to the system are approved. [d] Physical access restrictions associated with changes to the system are enforced. [e] Logical access restrictions associated with changes to the system are defined. [f] Logical access restrictions associated with changes to the system are documented. [g] Logical access restrictions associated with changes to the system are approved. [h] Logical access restrictions associated with changes to the system are enforced.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
Covered	[a] Access to CUI via essential programs are defined by Anchor authorized applications. [b] The use of non-essential programs to access CUI is not permitted. [c] The use of nonessential programs to access CUI is restricted by Anchor.
Customer Responsibility	[d] Essential functions are defined. [e] The use of nonessential functions is defined. [f] The use of nonessential functions is restricted, disabled, or prevented as defined. [g] Essential ports are defined. [h] The use of nonessential ports is defined. [i] The use of nonessential ports is restricted, disabled, or prevented as defined. [j] Essential protocols are defined. [k] The use of nonessential protocols is defined.

	[l] The use of nonessential protocols is restricted, disabled, or prevented as defined. [m] Essential services are defined. [n] The use of nonessential services is defined. [o] The use of nonessential services is restricted, disabled, or prevented as defined.
CM.3.069	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
Covered	[a] Application whitelisting is implemented for CUI access. [b] The software allowed to execute under whitelisting is specified by authorized applications in the Anchor CUI User Role. [c] Anchor prevents unauthorized applications from accessing CUI files.

Identification and Authentication (IA)

IA.1.076	Identify information system users, processes acting on behalf of users, or devices.
Shared responsibility	[a] Organization is responsible for specifying the CUI group and populating the group in the active directory or as a separate list. Anchor enforces the subsequent authentication for access. [b] Processes acting on behalf of users are identified by authorized applications in the Anchor User Role. [c] Devices accessing the system are identified by Anchor agents.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Covered	[a] The identity of each user is authenticated or verified by Anchor as a prerequisite to accessing CUI. [b] The identity of each process acting on behalf of a user is verified by Anchor as a prerequisite to accessing CUI. [c] The identity of each device accessing CUI is authenticated by the unique Anchor agent certificate as a prerequisite to accessing CUI.
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.

Customer Responsibility	[a] Password complexity requirements are defined. [b] Password change of character requirements are defined. [c] Minimum password complexity requirements as defined are enforced when new passwords are created. [d] Minimum password change of character requirements as defined are enforced when new passwords are created.
IA.2.079	Prohibit password reuse for a specified number of generations.
Customer Responsibility	[a] The number of generations during which a password cannot be reused is specified. [b] Reuse of passwords is prohibited during the specified number of generations.
IA.2.080	Allow temporary password use for system logons with an immediate change to a permanent password.
Customer Responsibility	[a] An immediate change to a permanent password is required when a temporary password is used for system logon.
IA.2.081	Store and transmit only cryptographically-protected passwords.
Customer Responsibility	[a] Passwords are cryptographically protected in storage. [b] Passwords are cryptographically protected in transit.
IA.2.082	Obscure feedback of authentication information.
Customer Responsibility	[a] Authentication information is obscured during the authentication process.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
Customer Responsibility	[a] Privileged accounts are identified. [b] Multifactor authentication is implemented for local access to privileged accounts. [c] Multifactor authentication is implemented for network access to privileged accounts. [d] Multifactor authentication is implemented for network access to non-privileged accounts.
IA.3.084	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
Customer Responsibility	[a] Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

IA.3.085	Prevent reuse of identifiers for a defined period.
Customer Responsibility	[a] A period within which identifiers cannot be reused is defined. [b] Reuse of identifiers is prevented within the defined period.

IA.3.086	Disable identifiers after a defined period of inactivity.
Customer Responsibility	[a] A period of inactivity after which an identifier is disabled is defined. [b] Identifiers are disabled after the defined period of inactivity.

Incident Response (IR)

IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
Customer Responsibility	[a] An operational incident-handling capability is established. [b] The operational incident-handling capability includes preparation. [c] The operational incident-handling capability includes detection. [d] The operational incident-handling capability includes analysis. [e] The operational incident-handling capability includes containment. [f] The operational incident-handling capability includes recovery. [g] The operational incident-handling capability includes user response activities.
IR.2.093	Detect and report events.
Customer Responsibility	[a] The organization has a process for identifying methods for event detection. [b] The organization can provide a process for reporting events so that they can be triaged, analyzed, and addressed.

IR.2.094	Analyze and triage events to support event resolution and incident declaration.
Customer Responsibility	[a] The organization analyzes events. [b] The organization performs correlation analysis on events. [c] The organization assigns a disposition to events. [d] The organization provides a process for reporting events so that they can be triaged, analyzed, and addressed. [e] The organization escalates events to the appropriate stakeholders, as needed.

IR.2.096	Develop and implement responses to declared incidents according to predefined procedures.
Customer Responsibility	[a] The organization has an incident declaration process. [b] The organization has predefined procedures that address incident response activities.

IR.2.097	Perform root cause analysis on incidents to determine underlying causes.
Customer Responsibility	[a] The organization has a post-incident response activity. [b] The organization determines the root cause of incidents.
IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
Customer Responsibility	[a] Incidents are tracked. [b] Incidents are documented. [c] Authorities to whom incidents are to be reported are identified. [d] Organizational officials to whom incidents are to be reported are identified. [e] Identified authorities are notified of incidents. [f] Identified organizational officials are notified of incidents.

IR.3.099	Test the organizational incident response capability.
Customer Responsibility	[a] The incident response capability is tested.

Maintenance (MA)

MA.2.111	Perform maintenance on organizational systems.
Customer Responsibility	[a] System maintenance is performed.
MA.2.112	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
Customer Responsibility	[a] Tools used to conduct system maintenance are controlled. [b] Techniques used to conduct system maintenance are controlled. [c] Mechanisms used to conduct system maintenance are controlled. [d] Personnel used to conduct system maintenance are controlled.

MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
Customer Responsibility	[a] Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections. [b] Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.
MA.2.114	Supervise the maintenance activities of maintenance personnel without required access authorization.
Customer Responsibility	[a] Maintenance personnel without required access authorization are supervised during maintenance activities.

MA.3.115	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
Customer Responsibility	[a] Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.
MA.3.116	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
Customer Responsibility	[a] 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)

MP.1.118	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
Covered	[a] Files containing FCI on system media are encrypted at rest. No usable data is retrievable. [b] Files containing FCI on system media are encrypted at rest. No usable data is retrievable.
MP.2.119	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
Customer Responsibility	[a] Paper media containing CUI is physically controlled. [b] Digital media containing CUI is physically controlled. [c] Paper media containing CUI is securely stored. [d] Digital media containing CUI is securely stored.

MP.2.120	Limit access to CUI on system media to authorized users.
Covered	[a] Access to CUI on system media is limited to authorized users by Anchor.
MP.2.121	Control the use of removable media on system components.
Covered	[a] All CUI files are anchored and therefore encrypted at rest. Copies made on removable media are unusable.

MP.3.122	Mark media with necessary CUI markings and distribution limitations.
Customer Responsibility	[a] Media containing CUI is marked with applicable CUI markings. [b] Media containing CUI is marked with distribution limitations.
MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.
Customer Responsibility	[a] The use of portable storage devices is prohibited when such devices have no identifiable owner.

MP.3.124	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
Customer Responsibility	[a] Access to media containing CUI is controlled. [b] Accountability for media containing CUI is maintained during transport outside of controlled areas.
MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
Covered	[a] CUI files are anchored and therefore encrypted with FIPS-validated Microsoft CNG.

Physical Protection (PE)

PE.1.131	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
Customer Responsibility	[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. [d] Physical access to operating environments is limited to authorized individuals.
PE.1.132	Escort visitors and monitor visitor activity.
Customer Responsibility	[a] Visitors are escorted. [b] Visitor activity is monitored.

PE.1.133	Maintain audit logs of physical access.
Customer Responsibility	[a] Audit logs of physical access are maintained.
PE.1.134	Control and manage physical access devices.
Customer Responsibility	[a] Physical access devices are identified. [b] Physical access devices are controlled. [c] Physical access devices are managed.

PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.
Customer Responsibility	[a] The physical facility where organizational systems reside is protected. [b] The support infrastructure for organizational systems is protected. [c] The physical facility where organizational systems reside is monitored. [d] The support infrastructure for organizational systems is monitored.
PE.3.136	Enforce safeguarding measures for CUI at alternate work sites.
Customer Responsibility	[a] Safeguarding measures for CUI are defined for alternate work sites. [b] Safeguarding measures for CUI are enforced for alternate work sites.

Personnel Security (PS)

PS.2.127	Screen individuals prior to authorizing access to organizational systems containing CUI.
Customer Responsibility	[a] Individuals are screened prior to authorizing access to organizational systems containing CUI.

PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
Covered	[a] When an employee is terminated all devices are returned. [b] When an employee is terminated their CUI file is revoked by Anchor. [c] By revoking access with Anchor the former employee can no longer access CUI files on devices they still have access to.

Recovery (RE)

RE.2.137	Regularly perform and test data backups.
Customer Responsibility	[a] A frequency to perform backups has been defined. [b] Backups are performed according to the defined backup schedule. [c] A frequency to test backups has been defined. [d] Backups are tested according to a defined test schedule. [e] Tests of backups include performing a restore that ensures a successful recovery. [f] Backup data is protected from a direct attack and from corruption by an attack against the primary data source.
RE.2.138	Protect the confidentiality of backup CUI at storage locations.
Covered	[a] CUI files are anchored and therefore encrypted at rest with a FIPS-validated module before it is copied to backup systems.

RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.
Customer Responsibility	[a] The organization automates its backups where feasible. [b] The organization has defined its requirements for the length of time needed to restore resources from backup (recovery time objectives (RTO)), the amount of time between backups (recovery point objectives (RPO)), and the length of time backups need to be retained. [c] Backup schedules and selection lists reflect documented organization requirements. [d] Key systems are backed up in a manner that enables rapid recovery, such as imaging.

Risk Management (RM)

RM.2.141	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
Customer Responsibility	[a] The frequency to assess risk to organizational operations, organizational assets, and individuals is defined. [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.
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
Customer Responsibility	[a] The frequency to scan for vulnerabilities in organizational systems and applications is defined. [b] Vulnerability scans are performed on organizational systems with the defined frequency. [c] Vulnerability scans are performed on applications with the defined frequency. [d] Vulnerability scans are performed on organizational systems when new vulnerabilities are identified. [e] Vulnerability scans are performed on applications when new vulnerabilities are identified.

RM.2.143	Remediate vulnerabilities in accordance with risk assessments.
Customer Responsibility	[a] Vulnerabilities are identified. [b] Vulnerabilities are remediated in accordance with risk assessments.
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
Customer Responsibility	[a] The organization maintains a process for performing risk assessments. [b] The organization documents and maintains defined risk categories, risk sources, and risk measurement criteria. [c] The organization prioritizes risk. [d] The organization performs risk assessment at a frequency defined by the organization.

RM.3.146	Develop and implement risk mitigation plans.

Customer Responsibility	[a] The organization develops an approach for mitigating each identified risk. [b] The organization implements risk mitigation plans for each identified risk.
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.
Customer Responsibility	[a] The organization maintains a list of products the organization is using that are no longer supported by their vendors or do not have any type of vendor support. [b] The organization documents how it manages the risk of each such product within the organization. [c] The organization tracks the risks of using non-vendor-supported products.

Situational Awareness (SA)

SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
Customer Responsibility	[a] The organization identifies cyber threat intelligence from information sharing forums and sources. [b] The organization responds to cyber threat intelligence from information sharing forums and sources. [c] The organization communicates this information to appropriate stakeholders.

System & Communications Protection (SC)

SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
Covered	[a] The external system boundary is defined as the set of PCs with Anchor software and the CUI role. [b] A key internal system boundary is defined as the Windows processes running Anchor authorized applications.
Shared Coverage	[d] Communications are partially monitored at the internal boundary. The level of monitoring depends on the application. [f] Communications are partially controlled at the internal boundary. The level of control depends on the application.

	[h] Communications are partially protected at the internal boundary. The level of protection depends on the application
Customer Responsibility	[c] Communications are monitored at the external system boundary. [e] Communications are controlled at the external system boundary. [h] Communications are protected at key internal boundaries.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
Shared Coverage	For CUI systems in the security architecture, there are no publicly accessible system components. For all other systems, customer is responsible for the segmentation.
SC.2.178	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
Customer Responsibility	[a] Collaborative computing devices are identified. [b] Collaborative computing devices provide indication to users of devices in use. [c] Remote activation of collaborative computing devices is prohibited.
SC.2.179	Use encrypted sessions for the management of network devices.
Customer Responsibility	[a] The organization has one or more policies and/or procedures for establishing connections to manage network devices. [b] The tools used for establishing remote connections to network devices use encryption.
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
Covered	[a] Anchor encrypts CUI with the FIPS-validated Microsoft Windows CNG module.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
Customer Responsibility	[a] Architectural designs that promote effective information security are identified. [b] Software development techniques that promote effective information security are identified. [c] Systems engineering principles that promote effective information security are identified.

	[d] Identified architectural designs that promote effective information security are employed. [e] Identified software development techniques that promote effective information security are employed. [f] Identified systems engineering principles that promote effective information security are employed.
SC.3.181	Separate user functionality from system management functionality.
Customer Responsibility	[a] User functionality is identified. [b] System management functionality is identified. [c] User functionality is separated from system management functionality.
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.
Covered	[a] Anchor scrubs residual FCI/CUI from system memory before files are closed. FCI/CUI on disk is always encrypted.
SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
Customer Responsibility	[a] Network communications traffic needs to be denied by default to through the firewall on each device in the system. There is no physical network within the system boundary. [b] Each device's firewall is configured to only allow traffic by exception.
SC.3.184	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
Shared Responsibility	In the security architecture, external connections are recommended to be blocked on system devices.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
Covered	[a] Anchor is used to prevent unauthorized disclosure of CUI. [c] Files containing CUI are always anchored during transmission to prevent unauthorized disclosure of CUI.
Shared Coverage	[b] There are no alternative physical safeguards intended to prevent unauthorized disclosure of CUI.

SC.3.186	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
Customer Responsibility	The proposed security architecture recommends that Windows is configured such that: [a] A period of inactivity to terminate network connections associated with communications sessions is defined. [b] Network connections associated with communications sessions are terminated at the end of the sessions. [c] Network connections associated with communications sessions are terminated after the defined period of inactivity.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.
Covered	[a] Anchor generates a unique cryptographic key for each anchored file. [b] Anchor manages cryptographic keys securely and automatically.
SC.3.188	Control and monitor the use of mobile code.
Customer Responsibility	[a] Use of mobile code is controlled. [b] Use of mobile code is monitored.
SC.3.189	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
Customer Responsibility	[a] Use of Voice over Internet Protocol (VoIP) technologies is controlled. [b] Use of Voice over Internet Protocol (VoIP) technologies is monitored.
SC.3.190	Protect the authenticity of communications sessions.
Customer Responsibility	[a] The authenticity of communications sessions is protected.
SC.3.191	Protect the confidentiality of CUI at rest.
Covered	[a] CUI is only stored in anchored files, which are encrypted at rest with FIPS-validated cryptography.
SC.3.192	Implement Domain Name System (DNS) filtering services.
Customer Responsibility	[a] The organization uses a DNS filtering service. [b] The organization has configured the enterprise to ensure outgoing web access requests utilize the DNS filtering service. [c] The organization monitors the DNS filtering service for effectiveness.

SC.3.193	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).
Customer Responsibility	[a] The organization has a security policy which restricts publishing CUI to any externally owned, publicly accessible information system. [b] The organization designates individuals authorized to post organization information onto any externally owned, publicly accessible information systems. [c] The organization trains authorized individuals to ensure that publicly accessible organization information does not contain CUI. [d] The organization conducts reviews to ensure CUI is not included in proposed content to be posted by the organization on a publicly accessible information system under its control. [e] The organization removes CUI, if discovered, from any publicly accessible information system under its control.

System and Information Integrity (SI)

SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.
Customer Responsibility	[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] System flaws are corrected within the specified time frame.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.
Customer Responsibility	[a] Designated locations for malicious code protection are identified. [b] Protection from malicious code at designated locations is provided.
SI.1.212	Update malicious code protection mechanisms when new releases are available.
Customer Responsibility	[a] Malicious code protection mechanisms are updated when new releases are available.

SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
Customer Responsibility	[a] The frequency for malicious code scans is defined. [b] Malicious code scans are performed with the defined frequency. [c] Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.
SI.2.214	Monitor system security alerts and advisories and take action in response.
Customer Responsibility	[a] Response actions to system security alerts and advisories are identified. [b] System security alerts and advisories are monitored. [c] Actions in response to system security alerts and advisories are taken.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
Customer Responsibility	[a] The system is monitored to detect attacks and indicators of potential attacks. [b] Inbound communications traffic is monitored to detect attacks and indicators of potential attacks. [c] Outbound communications traffic is monitored to detect attacks and indicators of potential attacks.
SI.2.217	Identify unauthorized use of organizational systems.
Customer Responsibility	[a] Authorized use of the system is defined. [b] Unauthorized use of the system is identified.
SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.
Customer Responsibility	[a] The organization employs spam protection mechanisms at information system entry points to detect unsolicited messages. [b] The organization employs spam protection mechanisms at information system entry points to take organizationally defined actions on unsolicited messages. [c] The organization employs spam protection mechanisms at information system exit points to detect unsolicited messages. [d] The organization employs spam protection mechanisms at information system exit points to take organizationally defined actions on unsolicited messages.

	[e] The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Conclusion

This document introduced the CMMC and its key points at high level. It described a model security architecture based on Anchor and Windows 10/11 that applies to a broad range of Department of Defense contractors and their business environments. Finally, it mapped the CMMC 2.0 Level 2 practices to the model Anchor Security Architecture and provided templates that can be used when creating your organization's SSP, reducing the time and effort to get CMMC 2.0 Level 2 certification.