POSITION PAPER SERIES

Evaluating Inheritable Practices by Service Providers

DISCLAIMER

The C3PAO Stakeholder Forum is an industry group of C3PAOs. The group is formed from C3PAOs and aspiring C3PAOs; it is open to all CMMC-AB Marketplace C3PAOs and confirmed C3PAO applicants. The mission is to advance the CMMC assessor and C3PAO input, participation, and consensus within the CMMC ecosystem. This include advocating for policies, sharing perspectives and working alongside the DoD, CMMC-AB, Organizations seeking certification and other stakeholders to advance the mission of CMMC, which broadly is to increase the cyber posture of the Defense Industrial Base. The C3PAO Stakeholder Forum's participation is voluntary and those individuals that participate do so of their own volition and without compensation. The views of the board and the C3PAO Stakeholder Forum are not necessarily those of each member or their respective companies. The DoD, and where delegated by the DoD to the CMMC-AB, are the ultimate authority with regard to CMMC. Any guidance contained within is not authoritative and if found in conflict with DoD guidance should be considered subordinate. We simply seek to share this guidance to help advance the conversations and drive consistency among the industry. To the extent that subsequent guidance is published by the DoD or similar authorities, this document will be revised.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

PURPOSE

Small service providers support multiple Organizations Seeking Certification (OSCs). These providers are requesting CMMC assessment of the practices they perform on behalf of their client OSC. C3PAOs need a standard method to perform CMMC assessment of providers so that the assessment can be recognized as evidence for client OSCs.

TERMS

CUI	Controlled Unclassified Information
CMMC	Cybersecurity Maturity Model Certification, a third-party assessment program which verifies that defense contractors with Controlled Unclassified Information meet NIST SP 800-171 requirements for security.
FedRAMP	Federal Risk and Authorization Management Program, a third-party assessment program which verifies that cloud service providers used by the Federal Government meet NIST SP 800-53 requirements for security.
C3PAO	CMMC Third Party Assessment Organization
CMMC-AB	CMMC Accreditation Body
DoD	United States Department of Defense, specifically the CMMC Program Management Office
OSC	Organization Seeking Certification – an entity which needs a CMMC Certificate in order to participate in DoD contracts.
Client OSC	An OSC which has at least one CMMC-required security function provided by the service provider. The service provider has requested CMMC assessment in order to provide inheritable evidence of compliance when the client OSC is assessed for CMMC certification.
Service provider	An external organization which performs CMMC-required security functions on behalf of an OSC, in order to protect CUI.
Small service provider	Private cloud hosts, Managed Service Providers (MSPs), and Managed Security Service Providers (MSSPs).
MSP	Service provider which typically fulfills the role of an in-house Information Technology department. This often includes a wide range of maintenance, access control, engineering, cybersecurity, malware protection, and backup services. MSPs often perform the majority of CMMC practices on behalf of their clients.
MSSP	Service provider which typically provides Security Operations Center services such as audit log management, incident detection, and incident response. MSSPs often perform a small sub-set of CMMC practices on behalf of their clients.
Private cloud	Service provider which typically performs storage, processing, or transmission of client data. This data may include CUI. Private clouds often perform all CMMC practices internally (to protect client CUI that their systems are hosting) as well as additional CMMC practices on behalf of their clients.
Shared Responsibility Matrix	A document which describes the service provider, the standard service that is available to client OSCs, and a per-Assessment Objective description of which organization is responsible for performance of each Assessment Objective.
Model client	A representative client OSC of the service provider. This model client must use the service listed in the Shared Responsibility Matrix. If no clients of the provider meet this description, a test or demonstration client may be used for assessment purposes.
ISO	International Standards Organization

DISCUSSION

PROBEM STATEMENT

- C3PAOs lack an industry-recognized method to perform an inheritable CMMC assessment of service providers.

DISCUSSION

- Small service providers such as private cloud hosts, Managed Service Providers (MSPs), and Managed Security Service Providers (MSSPs) may have dozens of client OSCs which use the same service offering. It is inefficient, costly, and redundant to have the same services fully assessed during each client OSC's assessment. If the small service provider can be assessed a single time to show that they are performing applicable CMMC practices on behalf of their clients, it will reduce the cost and risk for each client OSC's assessment.
- Client OSCs need assurance that their provider is capable of protecting CUI and will help them achieve CMMC certification before they choose a provider.
- The CMMC Assessment Process lacks guidance to perform standalone assessment of a service provider that performs some practices on behalf of an OSC.
- FedRAMP authorization is meant for cloud providers which provide services to the Federal Government. Small service providers are often ineligible or unable to obtain FedRAMP authorization because they do not host cloud services for the government.
- In addition, FedRAMP assessments utilize a much more comprehensive compliance standard than CMMC Level 2. FedRAMP moderate baseline includes a balance of NIST SP 800-53 controls which are appropriate for federal organizations. In contrast, CMMC contains a tailored set of NIST SP 800-53 controls which are appropriate for protecting confidentiality of CUI by nonfederal organizations. Using FedRAMP moderate baseline for all small providers introduces significant burden compared to CMMC assessment.
- The concept behind FedRAMP, however, is ideally suited for assessing service providers because it acknowledges the need to validate both the provider's internal security as well as validating security performed on behalf of the client. This position paper incorporates the proven methodology used by FedRAMP for provider assessment.
- C3PAOs and assessors need to be able to trust the veracity of CMMC assessments. By requiring CMMC credentials for assessors and their organizations, and providing a

standard process to use, assessments by authorized C3PAOs will be acceptable as evidence during OSC assessments.

PROPOSED WAY AHEAD

- C3PAOs and CMMC Assessors utilize recommended guidance within this paper to perform third party assessment of service providers. If this guidance is followed, the resulting Assessment Report and Shared Responsibility Matrix should be considered acceptable as evidence for client OSC's assessments
- We urge the Department of Defense to consider the process laid out in this paper as the foundation of a CMMC program for defense industrial base service providers, similar to the FedRAMP program for federal cloud service providers.
- If guidance from the Department of Defense is released which contradicts any portion of this position paper, this position paper will be revised as appropriate to match guidance.

RECOMMENDATION

HOW TO PERFORM CMMC ASSESSMENT OF SERVICE PROVIDERS

1. In order for the resulting assessment report to be considered eligible as evidence for future CMMC assessments, the C3PAO and CMMC assessment staff which perform the provider assessment must meet all CMMC Accreditation Body and Department of Defense requirements to perform CMMC assessments for certification. I.e., the C3PAO and all assessment team members will be listed on the CMMC-AB Marketplace in good standing at the time of assessment.

2. The service provider will provide a final Shared Responsibility Matrix during the assessment planning process.

    a. The Shared Responsibility Matrix will identify which CMMC Assessment Objectives are performed by the service provider on behalf of the client, and which are performed by the client. If an Assessment Objective is partially performed with some customer responsibilities, the service provider will describe the delineation of responsibilities in the spaces provided.

    b. The Shared Responsibility Matrix template from Appendix B is recommended for standardization purposes.

    c. An abbreviated example of a filled out Shared Responsibility Matrix is provided in Appendix A.

3. The service provider will identify a “model client” which utilizes the service offering described in the Shared Responsibility Matrix. If the service provider has current CMMC clients, they will select one of their existing clients as their “model client”. If the service provider has no existing CMMC clients, they may use a test or demonstration client to replicate the expected client activity and configurations.

4. The service provider must attest that the Shared Responsibility Matrix accurately describes the standard service provided to the “model client” and to their other CMMC clients. The assessment team is encouraged to perform spot checks of services provided to the other CMMC clients to verify this.

    a. Non-standard services which vary from client to client will not be included in the provider’s assessment. The provider will need to participate in each client OSC’s assessment to provide evidence for non-standard services performed on behalf of client OSCs.

    b. If the service provider has multiple “tiered” service offerings, i.e., a more advanced service includes basic services, a single Shared Responsibility Matrix may be used to describe multiple tiers within the same document. The C3PAO will require that the Shared Responsibility Matrix clearly describes responsibilities for each service tier such that a client will not be confused, prior

to accepting the engagement. Assessment reports for previously assessed services may be used as evidence to prevent duplication of effort for additional services. All services described within a single Shared Responsibility Matrix will be assessed as part of a single engagement.

c. If the service provider has multiple service discrete offerings being assessed, the assessing C3PAO will perform separate engagements for each service with separate Shared Responsibility Matrixes for each service offering. Assessment reports for previously assessed services may be used as evidence to prevent duplication of effort for additional services.

5. The service provider must attest that the assets they use to support the "model client" are managed using the same policy, processes, and practices as assets used for their other CMMC clients. The assessment team is encouraged to perform spot checks of services provided to the other CMMC clients to verify this.

6. Using the "model client", identify in-scope assets and applicable practices within the service provider.[1]

   a. If the service provider stores, processes, or transmits CUI on behalf of the client, the location and data flows for that CUI will be used to identify in-scope assets within the provider's information system. The provider will be assessed to verify that they are performing all applicable CMMC practices to protect client CUI within their organization.

   b. If the service provider performs a security function on behalf of the client, the systems used to provide that security function will be identified as in-scope assets and assessed against applicable practices for external Security Protection Assets.

   c. Note: The "model client" is not expected to participate in the service provider's assessment and will not receive a CMMC certification as part of this engagement. The purpose of identifying a "model client" is to provide clarity for scoping and shared responsibilities.

7. In addition to the assessment of in-scope assets, the service provider will be assessed to verify that they are performing the provider responsibilities as described in the Shared Responsibility Matrix. This portion of the assessment will be performed from the perspective of the "model client", as though the "model client" had requested a CMMC assessment for themselves.

8. The assessment of the service provider will be conducted by the C3PAO as an ISO 17020 Certification Body following the CMMC Assessment Process.

9. The C3PAO will attach the Shared Responsibility Matrix to the assessment report as an appendix.

[1] Reference CMMC Scoping Scenarios Analysis (Scenario 12) for analysis of scoping from the client's perspective.

a. In order to be eligible for use as evidence during a client OSC's assessment[2], the assessment report must include 1) a description of the service provider's internal scope; 2) which practices and assessment objectives were evaluated as applicable to the service provider; 3) which practices and assessment objectives were determined MET, NOT MET, or NOT APPLICABLE; and 4) attestation that practices performed on behalf of the client OSC are accurately described in the Shared Responsibility Matrix.

10. No CMMC certificate will be issued to the service provider.[3]

    a. Because service providers are considered supporting units by the CMMC Assessment Process, which are ineligible for certification, service provider assessment is ineligible for CMMC certification.

    b. The process described in this paper is for service providers who perform CMMC requirements on behalf of their client OSCs. The client OSC remains ultimately responsible for the security of their CUI and information systems.

    c. If the service provider is seeking a CMMC certificate for eligibility to participate in DoD contracts and is performing CMMC requirements to protect their own CUI, they should seek a standard CMMC assessment.

11. The assessment report and Shared Responsibility Matrix may be provided to the service provider's clients (and prospective clients) by the service provider. The assessment report may be used as evidence for CMMC assessment of OSCs that inherit protections from the service provider.

[2] It is vital that sufficient information is included to identify which assessment objectives, practices, and scope were validated during the service provider's assessment.
[3] Long term, we would like to see the DoD authorize a CMMC certification which is specific to service providers who provide services to defense contractors.

HOW TO VERIFY NON-DUPLICATION FROM SERVICE PROVIDER ASSESSMENT REPORTS

The following steps will be performed during the planning stage of the CMMC assessment by the lead assessor.

1. The lead assessor will validate that the C3PAO and CMMC assessment staff which performed the provider assessment have met all CMMC Accreditation Body and Department of Defense requirements to perform CMMC assessments for certification.

2. The lead assessor will review the client OSC's proposed scope and validate that the client OSC is utilizing the exact service described in the Shared Responsibility Matrix.

3. The lead assessor will verify that the provider's assessment report was issued within 3 years of the client OSC's planned assessment date.[4]

4. The lead assessor may choose to perform spot checks of the service provider at their discretion. The client OSC will be obligated to request participation from the service provider during the planning phase as requested to:

    a. validate that the "model client" used for the provider assessment is representational of the client OSC's use of services; and

    b. validate that the service provider's policy, processes, and practices have not significantly changed since the provider's assessment.

5. The customer responsibilities as described in the Shared Responsibility Matrix will be included in the assessment plan to ensure they are performed by the client OSC.

6. Upon satisfactorily determining that the provider's assessment report is accurate and was performed by authorized CMMC assessors, the lead assessor may choose to accept the assessment report as evidence for performance of CMMC practices by the service provider, following the CMMC Assessment Procedure for non-duplication.

7. If the lead assessor determines that the provider's assessment report is not acceptable for non-duplication, the lead assessor will notify the OSC and C3PAO during the assessment planning stage. The OSC will be responsible for coordinating participation from the service provider as necessary to provide evidence during the assessment.

[4] We received feedback from several CMMC Provisional Assessors that assessment reports become less trustworthy over time (due to risk that the provider will change their system or will stop performing security controls). We are concerned that assessors will encounter occasional issues with expiring reports in the middle of OSC assessments. Finally, client OSCs should have as much notice as possible if their service provider fails their assessment. For these reasons, we recommend re-assessment of service providers on an 18-month schedule.

SUPPLEMENTARY INFORMATION

CMMC Assessment Guide

The CMMC Assessment Guide for Level 2 discusses inheritance. It states that a practice objective is MET if adequate evidence is presented that the service provider performs the practice objective.

> A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. An ESP may be external people, technology, or facilities that the contractor uses, including cloud service providers, managed service providers, managed security service providers, cybersecurity-as-a-service providers.
>
> Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice.

Non-duplication

The CMMC Assessment Process describes non-duplication. Non-duplication allows for an assessor to accept recent third-party assessment records as sole evidence of performance of practice objectives, rather than requiring the assessor to repeat the Examine / Interview / Test for those practice objectives.

NIST definition of Control Inheritance

"A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See common control."[5]

NIST definition of Common Control

"A security or privacy control that is inherited by multiple information systems or programs."[6]

[5] NIST Special Publication 800-53 Revision 5
[6] NIST Special Publication 800-53 Revision 5

NIST definition of Hybrid Control

"A security control that is implemented in an information system in part as a common control and in part as a system-specific control."[7]

NIST SP 800-53 Rev.5 instructions for Common Controls

"Common controls are controls whose implementation results in a capability that is inheritable by multiple systems or programs. A control is deemed inheritable when the system or program receives protection from the implemented control, but the control is developed, implemented, assessed, authorized, and monitored by an internal or external entity other than the entity responsible for the system or program. The security and privacy capabilities provided by common controls can be inherited from many sources, including mission or business lines, organizations, enclaves, environments of operation, sites, or other systems or programs. Implementing controls as common controls can introduce the risk of a single point of failure."[8]

"Many of the controls needed to protect organizational information systems—including many physical and environmental protection controls, personnel security controls, and incident response controls—are inheritable and, therefore, are good candidates for common control status. Common controls can also include technology-based controls, such as identification and authentication controls, boundary protection controls, audit and accountability controls, and access controls. The cost of development, implementation, assessment, authorization, and monitoring can be amortized across multiple systems, organizational elements, and programs using the common control implementation approach."[9]

"Organizations can implement a control as hybrid if one part of the control is common (inheritable) and the other part is system-specific. For example, an organization may implement control CP-2 using a predefined template for the contingency plan for all organizational information systems with individual system owners tailoring the plan for system-specific uses, where appropriate. The division of a hybrid control into its common (inheritable) and system-specific parts may vary by organization, depending on the types of information technologies employed, the approach used by the organization to manage its controls, and assignment of responsibilities. When a control is implemented as a hybrid control, the common control provider is responsible for ensuring the implementation, assessment, and monitoring of the common part of the hybrid control, and the system owner is responsible for ensuring the implementation, assessment, and monitoring of the system-specific part of the hybrid control. Implementing controls as hybrid controls can

[7] NIST Special Publication 800-39
[8] NIST Special Publication 800-53 , Revision 5. Page 12
[9] NIST Special Publication 800-53 , Revision 5. Page 12

introduce risk if the responsibility for the implementation and ongoing management of the common and system-specific parts of the controls is unclear."[10]

Requirement for FedRAMP compliance

The topic of FedRAMP compliance is discussed here because OSCs have significant confusion about the regulatory requirements for defense contractor service providers.

The Department of Defense, using DFARS clause 252.204-7012, requires defense contractors to use FedRAMP moderate authorized (or equivalent) cloud service providers if they store, process, or transmit Covered Defense Information on those cloud systems.

However, cloud service providers as defined in DFARS are actually a narrow sub-set of all service providers. The service providers discussed in this paper would not be required to have FedRAMP moderate authorization (or equivalent) because they do not meet the DFARS definition of a cloud service provider.

Below is an excerpted question and answer from DoD CIO's office on January 27, 2022.

Question
"Regarding DFARS 252.204-7012 and the requirement "If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information…"

Can you confirm that the DoD uses the Essential Characteristics listed in NIST SP 800-145 "The NIST Definition of Cloud Computing" to determine whether an external provider is a Cloud Computing provider?"

Answer
"While DFARS 252.204-7012 does not include a definition for cloud computing, DoD does define it in DFARS clause 252.239-7010, Cloud Computing Services as:

""Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service."

Note that this definition includes the NIST definition for Cloud in NIST SP 800-145 as well as the NIST SP 800-145 Cloud 'Essential Characteristics": "on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service."

[10] NIST Special Publication 800-53 , Revision 5. Page 12

It is important to note that there is no precedent for requiring FedRAMP moderate (or equivalency) for small service providers such as MSPs or MSSPs.

CMMC assessment is more appropriate than the FedRAMP moderate baseline for small service providers that do not meet the essential characteristics of a cloud service provider per NIST SP 800-145. Requiring FedRAMP moderate baseline for all defense industrial base service providers imposes a significant burden on these providers and will greatly increase cost to both service providers and client OSCs compared to CMMC.

Cybersecurity expectations for external service providers

SA-9 from NIST SP 800-53 Revision 5 provides an excellent explanation of cybersecurity expectations for external service providers. SA-9 is also listed in NIST SP 800-171 Appendix E as a control expected to be performed by non-federal organizations without specification.

SA-9 EXTERNAL SYSTEM SERVICES

Control:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [*Assignment: organization-defined controls*];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [*Assignment: organization-defined processes, methods, and techniques*].

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. [11]

In order to ensure that providers of external system services comply with organizational security and privacy requirements, a third-party assessment is ideal. A third-party

[11] NIST SP 800-53 Revision 5, page 271

assessment performed by a C3PAO would be an examinable artifact for SA-9.[12] A third-party assessment performed by a C3PAO would also be acceptable for non-duplication as described in the CMMC Assessment Process.

For small service providers that have client OSCs subject to CMMC Level 2, a CMMC Level 2 assessment is appropriate. A CMMC assessment which validates applicable practices will provide assurance that the provider will not reduce the security posture of the defense industrial base client.

[12] NIST SP 800-53A Revision 5, page 480 lists "control assessment results or reports from external providers of system services" as a potential Examine object.

Appendix A – Example Shared Responsibility Matrix

SERVICE PROVIDER IDENTIFICATION

Service Provider Name	USA Managed Services Corp
Corporate address	123 Lincoln Lane, Washington DC, 21199, USA
CMMC point of contact (name, email, phone)	John Smith, john.smith@usamsc.us, 555-555-555
Country(s) hosting provided services and datacenters	United States of America
Are all support personnel U.S. persons?	Yes

SERVICE OFFERING

Service ID	Service name	Service description
CMMC-L2-MSP	System Management for CMMC Level 2	Systems management to support client's business needs. This service replaces a traditional IT department, with expertise in helpdesk, system administration, networking, cybersecurity, and systems engineering.

SHARED RESPONSIBILITY MATRIX

Practice ID	AO	AO Text	Provider Responsibility	Customer Responsibility
AC.L1-3.1.1	a	authorized users are identified;	No responsibility	Full responsibility
AC.L1-3.1.1	b	processes acting on behalf of authorized users are identified;	Full responsibility	No responsibility
AC.L1-3.1.1	c	devices (and other systems) authorized to connect to the system are identified;	Full responsibility	No responsibility

AC.L1-3.1.1	d	system access is limited to authorized users;	Full responsibility other than as described in customer responsibility	Responsible for notifying provider promptly when users are onboarded or offboarded.
AC.L1-3.1.1	e	system access is limited to processes acting on behalf of authorized users; and	Full responsibility	No responsibility
AC.L1-3.1.1	f	system access is limited to authorized devices (including other systems).	Full responsibility	No responsibility
AC.L1-3.1.2	a	the types of transactions and functions that authorized users are permitted to execute are defined;	Full responsibility	No responsibility
AC.L1-3.1.2	b	system access is limited to the defined types of transactions and functions for authorized users.	Full responsibility other than as described in customer responsibility	Responsible for notifying provider of desired transactions and functions for authorized users
AC.L1-3.1.20	a	connections to external systems are identified;	Full responsibility other than as described in customer responsibility	If connection to new external system is requested, submit Change Request
AC.L1-3.1.20	b	the use of external systems is identified;	Full responsibility	No responsibility
AC.L1-3.1.20	c	connections to external systems are verified;	Full responsibility	No responsibility
AC.L1-3.1.20	d	the use of external systems is verified;	Full responsibility	No responsibility
AC.L1-3.1.20	e	connections to external systems are controlled/limited; and	Full responsibility	No responsibility

Appendix B – Shared Responsibility Matrix Template

SERVICE PROVIDER IDENTIFICATION

Service Provider Name	
Corporate address	
CMMC point of contact (name, email, phone)	
Country(s) hosting provided services and datacenters	
Are all support personnel U.S. persons?	

SERVICE OFFERING

Service ID	Service name	Service description

SHARED RESPONSIBILITY MATRIX

Practice ID	AO	AO Text	Provider Responsibility	Customer Responsibility
AC.L1-3.1.1	a	authorized users are identified;		
AC.L1-3.1.1	b	processes acting on behalf of authorized users are identified;		

AC.L1-3.1.1	c	devices (and other systems) authorized to connect to the system are identified;		
AC.L1-3.1.1	d	system access is limited to authorized users;		
AC.L1-3.1.1	e	system access is limited to processes acting on behalf of authorized users; and		
AC.L1-3.1.1	f	system access is limited to authorized devices (including other systems).		
AC.L1-3.1.2	a	the types of transactions and functions that authorized users are permitted to execute are defined; and		
AC.L1-3.1.2	b	system access is limited to the defined types of transactions and functions for authorized users.		
AC.L1-3.1.20	a	connections to external systems are identified;		
AC.L1-3.1.20	b	the use of external systems is identified;		
AC.L1-3.1.20	c	connections to external systems are verified;		
AC.L1-3.1.20	d	the use of external systems is verified;		
AC.L1-3.1.20	e	connections to external systems are controlled/limited; and		
AC.L1-3.1.20	f	the use of external systems is controlled/limited.		
AC.L1-3.1.22	a	individuals authorized to post or process information on publicly accessible systems are identified;		
AC.L1-3.1.22	b	procedures to ensure FCI is not posted or processed on publicly accessible systems are identified;		

AC.L1-3.1.22	c	a review process is in place prior to posting of any content to publicly accessible systems;		
AC.L1-3.1.22	d	content on publicly accessible systems is reviewed to ensure that it does not include FCI; and		
AC.L1-3.1.22	e	mechanisms are in place to remove and address improper posting of FCI.		
AC.L2-3.1.10	a	the period of inactivity after which the system initiates a session lock is defined;		
AC.L2-3.1.10	b	access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and		
AC.L2-3.1.10	c	previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.		
AC.L2-3.1.11	a	conditions requiring a user session to terminate are defined; and		
AC.L2-3.1.11	b	a user session is automatically terminated after any of the defined conditions occur.		
AC.L2-3.1.12	a	remote access sessions are permitted;		
AC.L2-3.1.12	b	the types of permitted remote access are identified;		
AC.L2-3.1.12	c	remote access sessions are controlled; and		
AC.L2-3.1.12	d	remote access sessions are monitored.		
AC.L2-3.1.13	a	cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and		

AC.L2-3.1.13	b	cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.		
AC.L2-3.1.14	a	managed access control points are identified and implemented;		
AC.L2-3.1.14	a	privileged commands authorized for remote execution are identified;		
AC.L2-3.1.14	b	remote access is routed through managed network access control points.		
AC.L2-3.1.15	b	security-relevant information authorized to be accessed remotely is identified;		
AC.L2-3.1.15	c	the execution of the identified privileged commands via remote access is authorized; and		
AC.L2-3.1.15	d	access to the identified security-relevant information via remote access is authorized.		
AC.L2-3.1.16	a	wireless access points are identified; and		
AC.L2-3.1.16	b	wireless access is authorized prior to allowing such connections.		
AC.L2-3.1.17	a	wireless access to the system is protected using authentication; and		
AC.L2-3.1.17	b	wireless access to the system is protected using encryption.		
AC.L2-3.1.18	a	mobile devices that process, store, or transmit CUI are identified;		
AC.L2-3.1.18	b	mobile device connections are authorized; and		
AC.L2-3.1.18	c	mobile device connections are monitored and logged.		
AC.L2-3.1.19	a	mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and		

AC.L2-3.1.19	b	encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.		
AC.L2-3.1.21	a	the use of portable storage devices containing CUI on external systems is identified and documented;		
AC.L2-3.1.21	b	limits on the use of portable storage devices containing CUI on external systems are defined; and		
AC.L2-3.1.21	c	the use of portable storage devices containing CUI on external systems is limited as defined.		
AC.L2-3.1.3	a	information flow control policies are defined;		
AC.L2-3.1.3	b	methods and enforcement mechanisms for controlling the flow of CUI are defined;		
AC.L2-3.1.3	c	designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified;		
AC.L2-3.1.3	d	authorizations for controlling the flow of CUI are defined; and		
AC.L2-3.1.3	e	approved authorizations for controlling the flow of CUI are enforced.		
AC.L2-3.1.4	a	the duties of individuals requiring separation are defined;		
AC.L2-3.1.4	b	responsibilities for duties that require separation are assigned to separate individuals; and		
AC.L2-3.1.4	c	access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.		

AC.L2-3.1.5	a	privileged accounts are identified;		
AC.L2-3.1.5	b	access to privileged accounts is authorized in accordance with the principle of least privilege;		
AC.L2-3.1.5	c	security functions are identified; and		
AC.L2-3.1.5	d	access to security functions is authorized in accordance with the principle of least privilege.		
AC.L2-3.1.6	a	nonsecurity functions are identified; and		
AC.L2-3.1.6	b	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.		
AC.L2-3.1.7	a	privileged functions are defined;		
AC.L2-3.1.7	b	non-privileged users are defined;		
AC.L2-3.1.7	c	non-privileged users are prevented from executing privileged functions; and		
AC.L2-3.1.7	d	the execution of privileged functions is captured in audit logs.		
AC.L2-3.1.8	a	the means of limiting unsuccessful logon attempts is defined; and		
AC.L2-3.1.8	b	the defined means of limiting unsuccessful logon attempts is implemented.		
AC.L2-3.1.9	a	privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and		
AC.L2-3.1.9	b	privacy and security notices are displayed.		
AT.L2-3.2.1	a	security risks associated with organizational activities involving CUI are identified;		

AT.L2-3.2.1	b	policies, standards, and procedures related to the security of the system are identified;		
AT.L2-3.2.1	c	managers, systems administrators, and users of the system are made aware of the security risks associated with their activities; and		
AT.L2-3.2.1	d	managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.		
AT.L2-3.2.2	a	information security-related duties, roles, and responsibilities are defined;		
AT.L2-3.2.2	b	information security-related duties, roles, and responsibilities are assigned to designated personnel; and		
AT.L2-3.2.2	c	personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.		
AT.L2-3.2.3	a	potential indicators associated with insider threats are identified; and		
AT.L2-3.2.3	b	security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.		
AU.L2-3.3.1	a	audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified;		
AU.L2-3.3.1	b	the content of audit records needed to support monitoring, analysis,		

		investigation, and reporting of unlawful or unauthorized system activity is defined;		
AU.L2-3.3.1	c	audit records are created (generated);		
AU.L2-3.3.1	d	audit records, once created, contain the defined content;		
AU.L2-3.3.1	e	retention requirements for audit records are defined; and		
AU.L2-3.3.1	f	audit records are retained as defined.		
AU.L2-3.3.2	a	the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and		
AU.L2-3.3.2	b	audit records, once created, contain the defined content.		
AU.L2-3.3.3	a	a process for determining when to review logged events is defined;		
AU.L2-3.3.3	b	event types being logged are reviewed in accordance with the defined review process; and		
AU.L2-3.3.3	c	event types being logged are updated based on the review.		
AU.L2-3.3.4	a	personnel or roles to be alerted in the event of an audit logging process failure are identified;		
AU.L2-3.3.4	b	types of audit logging process failures for which alert will be generated are defined; and		
AU.L2-3.3.4	c	identified personnel or roles are alerted in the event of an audit logging process failure.		
AU.L2-3.3.5	a	audit record review, analysis, and reporting processes for investigation and response to indications of unlawful,		

		unauthorized, suspicious, or unusual activity are defined; and		
AU.L2-3.3.5	b	defined audit record review, analysis, and reporting processes are correlated.		
AU.L2-3.3.6	a	an audit record reduction capability that supports on-demand analysis is provided; and		
AU.L2-3.3.6	b	a report generation capability that supports on-demand reporting is provided.		
AU.L2-3.3.7	a	internal system clocks are used to generate time stamps for audit records;		
AU.L2-3.3.7	b	an authoritative source with which to compare and synchronize internal system clocks is specified; and		
AU.L2-3.3.7	c	internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.		
AU.L2-3.3.8	a	audit information is protected from unauthorized access;		
AU.L2-3.3.8	b	audit information is protected from unauthorized modification;		
AU.L2-3.3.8	c	audit information is protected from unauthorized deletion;		
AU.L2-3.3.8	d	audit logging tools are protected from unauthorized access;		
AU.L2-3.3.8	e	audit logging tools are protected from unauthorized modification; and		
AU.L2-3.3.8	f	audit logging tools are protected from unauthorized deletion.		

AU.L2-3.3.9	a	a subset of privileged users granted access to manage audit logging functionality is defined; and		
AU.L2-3.3.9	b	management of audit logging functionality is limited to the defined subset of privileged users.		
CA.L2-3.12.1	a	the frequency of security control assessments is defined; and		
CA.L2-3.12.1	b	security controls are assessed with the defined frequency to determine if the controls are effective in their application.		
CA.L2-3.12.2	a	deficiencies and vulnerabilities to be addressed by the plan of action are identified;		
CA.L2-3.12.2	a	security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.		
CA.L2-3.12.2	b	a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities; and		
CA.L2-3.12.2	c	the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.		
CA.L2-3.12.4	a	a system security plan is developed;		
CA.L2-3.12.4	b	the system boundary is described and documented in the system security plan;		
CA.L2-3.12.4	c	the system environment of operation is described and documented in the system security plan;		

CA.L2-3.12.4	d	the security requirements identified and approved by the designated authority as non-applicable are identified;		
CA.L2-3.12.4	e	the method of security requirement implementation is described and documented in the system security plan;		
CA.L2-3.12.4	f	the relationship with or connection to other systems is described and documented in the system security plan;		
CA.L2-3.12.4	g	the frequency to update the system security plan is defined; and		
CA.L2-3.12.4	h	system security plan is updated with the defined frequency.		
CM.L2-3.4.1	a	a baseline configuration is established;		
CM.L2-3.4.1	b	the baseline configuration includes hardware, software, firmware, and documentation;		
CM.L2-3.4.1	c	the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle;		
CM.L2-3.4.1	d	a system inventory is established;		
CM.L2-3.4.1	e	the system inventory includes hardware, software, and documentation; and		
CM.L2-3.4.1	f	the inventory is maintained (reviewed and updated) throughout the system development life cycle.		
CM.L2-3.4.2	a	security configuration settings for information technology products employed in the system are established and included in the baseline configuration; and		

CM.L2-3.4.2	b	security configuration settings for information technology products employed in the system are enforced.		
CM.L2-3.4.3	a	changes to the system are tracked;		
CM.L2-3.4.3	b	changes to the system are reviewed;		
CM.L2-3.4.3	c	changes to the system are approved or disapproved; and		
CM.L2-3.4.3	d	changes to the system are logged.		
CM.L2-3.4.4	a	the security impact of changes to the system is analyzed prior to implementation.		
CM.L2-3.4.5	a	physical access restrictions associated with changes to the system are defined;		
CM.L2-3.4.5	b	physical access restrictions associated with changes to the system are documented;		
CM.L2-3.4.5	c	physical access restrictions associated with changes to the system are approved;		
CM.L2-3.4.5	d	physical access restrictions associated with changes to the system are enforced;		
CM.L2-3.4.5	e	logical access restrictions associated with changes to the system are defined;		
CM.L2-3.4.5	f	logical access restrictions associated with changes to the system are documented;		
CM.L2-3.4.5	g	logical access restrictions associated with changes to the system are approved; and		
CM.L2-3.4.5	h	logical access restrictions associated with changes to the system are enforced.		

CM.L2-3.4.6	a	essential system capabilities are defined based on the principle of least functionality; and		
CM.L2-3.4.6	b	the system is configured to provide only the defined essential capabilities.		
CM.L2-3.4.7	a	essential programs are defined;		
CM.L2-3.4.7	b	the use of nonessential programs is defined;		
CM.L2-3.4.7	c	the use of nonessential programs is restricted, disabled, or prevented as defined;		
CM.L2-3.4.7	d	essential functions are defined;		
CM.L2-3.4.7	e	the use of nonessential functions is defined;		
CM.L2-3.4.7	f	the use of nonessential functions is restricted, disabled, or prevented as defined;		
CM.L2-3.4.7	g	essential ports are defined;		
CM.L2-3.4.7	h	the use of nonessential ports is defined;		
CM.L2-3.4.7	i	the use of nonessential ports is restricted, disabled, or prevented as defined;		
CM.L2-3.4.7	j	essential protocols are defined;		
CM.L2-3.4.7	k	the use of nonessential protocols is defined;		
CM.L2-3.4.7	l	the use of nonessential protocols is restricted, disabled, or prevented as defined;		
CM.L2-3.4.7	m	essential services are defined;		
CM.L2-3.4.7	n	the use of nonessential services is defined; and		
CM.L2-3.4.7	o	the use of nonessential services is restricted, disabled, or prevented as defined.		

CM.L2-3.4.8	a	a policy specifying whether whitelisting or blacklisting is to be implemented is specified;		
CM.L2-3.4.8	b	the software allowed to execute under whitelisting or denied use under blacklisting is specified; and		
CM.L2-3.4.8	c	whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.		
CM.L2-3.4.9	a	a policy for controlling the installation of software by users is established;		
CM.L2-3.4.9	b	installation of software by users is controlled based on the established policy; and		
CM.L2-3.4.9	c	installation of software by users is monitored.		
IA.L1-3.5.1	a	system users are identified;		
IA.L1-3.5.1	b	processes acting on behalf of users are identified; and		
IA.L1-3.5.1	c	devices accessing the system are identified.		
IA.L1-3.5.2	a	the identity of each user is authenticated or verified as a prerequisite to system access;		
IA.L1-3.5.2	b	the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and		
IA.L1-3.5.2	c	the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.		
IA.L2-3.5.10	a	passwords are cryptographically protected in storage; and		

IA.L2-3.5.10	b	passwords are cryptographically protected in transit.		
IA.L2-3.5.11	a	authentication information is obscured during the authentication process.		
IA.L2-3.5.3	a	privileged accounts are identified;		
IA.L2-3.5.3	b	multifactor authentication is implemented for local access to privileged accounts;		
IA.L2-3.5.3	c	multifactor authentication is implemented for network access to privileged accounts; and		
IA.L2-3.5.3	d	multifactor authentication is implemented for network access to non-privileged accounts.		
IA.L2-3.5.4	a	replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.		
IA.L2-3.5.5	a	a period within which identifiers cannot be reused is defined; and		
IA.L2-3.5.5	b	reuse of identifiers is prevented within the defined period.		
IA.L2-3.5.6	a	a period of inactivity after which an identifier is disabled is defined; and		
IA.L2-3.5.6	b	identifiers are disabled after the defined period of inactivity.		
IA.L2-3.5.7	a	password complexity requirements are defined;		
IA.L2-3.5.7	b	password change of character requirements are defined;		
IA.L2-3.5.7	c	minimum password complexity requirements as defined are enforced when new passwords are created;		

IA.L2-3.5.7	d	minimum password change of character requirements as defined are enforced when new passwords are created.		
IA.L2-3.5.8	a	the number of generations during which a password cannot be reused is specified and		
IA.L2-3.5.8	b	reuse of passwords is prohibited during the specified number of generations.		
IA.L2-3.5.9	a	an immediate change to a permanent password is required when a temporary password is used for system logon.		
IR.L2-3.6.1	a	an operational incident-handling capability is established;		
IR.L2-3.6.1	b	an operational incident-handling capability includes preparation;		
IR.L2-3.6.1	c	an operational incident-handling capability includes detection;		
IR.L2-3.6.1	d	an operational incident-handling capability includes analysis;		
IR.L2-3.6.1	e	an operational incident-handling capability includes containment;		
IR.L2-3.6.1	f	an operational incident-handling capability includes recovery; and		
IR.L2-3.6.1	g	an operational incident-handling capability includes user response activities.		
IR.L2-3.6.2	a	incidents are tracked;		
IR.L2-3.6.2	b	incidents are documented;		
IR.L2-3.6.2	c	authorities to whom incidents are to be reported are identified;		
IR.L2-3.6.2	d	organizational officials to whom incidents are to be reported are identified;		

IR.L2-3.6.2	e	identified authorities are notified of incidents; and		
IR.L2-3.6.2	f	identified organizational officials are notified of incidents.		
IR.L2-3.6.3	a	the incident resposne capability is tested.		
MA.L2-3.7.1	a	system maintenance is performed.		
MA.L2-3.7.2	a	tools used to conduct system maintenance are controlled;		
MA.L2-3.7.2	b	techniques used to conduct system maintenance are controlled;		
MA.L2-3.7.2	c	mechanisms used to conduct system maintenance are controlled; and		
MA.L2-3.7.2	d	personnel used to conduct system maintenance are controlled.		
MA.L2-3.7.3	a	equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.		
MA.L2-3.7.4	a	media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.		
MA.L2-3.7.5	a	multifactor authentication is used to establish nonlocal maintenance sessions via external network connections; and		
MA.L2-3.7.5	a	maintenance personnel without required access authorization are supervised during maintenance activities.		
MA.L2-3.7.5	b	nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.		

MP.L1-3.8.3	a	system media containing FCI is sanitized or destroyed before disposal; and		
MP.L1-3.8.3	b	system media containing FCI is sanitized before it is released for reuse.		
MP.L2-3.8.1	a	paper media containing CUI is physically controlled;		
MP.L2-3.8.1	b	digital media containing CUI is physically controlled;		
MP.L2-3.8.1	c	paper media containing CUI is securely stored; and		
MP.L2-3.8.1	d	digital media containing CUI is securely stored.		
MP.L2-3.8.2	a	access to CUI on system media is limited to authorized users.		
MP.L2-3.8.4	a	media containing CUI is marked with applicable CUI markings; and		
MP.L2-3.8.4	b	media containing CUI is marked with distribution limitations.		
MP.L2-3.8.5	a	access to media containing CUI is controlled; and		
MP.L2-3.8.5	b	accountability for media containing CUI is maintained during transport outside of controlled areas;		
MP.L2-3.8.6	a	the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.		
MP.L2-3.8.7	a	the use of removable media on system components is controlled.		
MP.L2-3.8.8	a	the use of portable storage devices is prohibited when such devices have no identifiable owner.		
MP.L2-3.8.9	a	the confidentiality of backup CUI is protected at storage locations.		

PE.L1-3.10.1	a	authorized individuals allowed physical access are identified;		
PE.L1-3.10.1	b	physical access to organizational systems is limited to authorized individuals;		
PE.L1-3.10.1	c	physical access to equipment is limited to authorized individuals; and		
PE.L1-3.10.1	d	physical access to operating environments is limited to authorized individuals.		
PE.L1-3.10.3	a	visitors are escorted; and		
PE.L1-3.10.3	b	visitor activity is monitored.		
PE.L1-3.10.4	a	audit logs of physical access are maintained.		
PE.L1-3.10.5	a	physical access devices are identified;		
PE.L1-3.10.5	b	physical access devices are controlled; and		
PE.L1-3.10.5	c	physical access devices are managed.		
PE.L2-3.10.2	a	the physical facility where organizational systems reside is protected;		
PE.L2-3.10.2	b	the support infrastructure for organizational systems is protected;		
PE.L2-3.10.2	c	the physical facility where organizational systems reside is monitored; and		
PE.L2-3.10.2	d	the support infrastructure for organizational systems is monitored.		
PE.L2-3.10.6	a	safeguarding measures for CUI are defined for alternative work sites; and		

PE.L2-3.10.6	b	safeguarding measures for CUI are enforced for alternative work sites.		
PS.L1-3.9.2	b	system access and credentials are terminated consistent with personnel actions such as termination or transfer; and		
PS.L1-3.9.2	c	the system is protected during and after personnel transfer actions.		
PS.L2-3.9.1	a	individuals are screened prior to authorizing access to organizational systems containing CUI.		
PS.L2-3.9.2	a	a policy and/or process for terminating system access and any credentials coincident with personnel actions is established;		
RA.L2-3.11.1	a	the frequency to assess risk to organizational operations, organizational assets, and individuals is defined; and		
RA.L2-3.11.1	b	risk to organizational operations, organizational assets, and individuals resulting from the operation of an orgaizational system that processes, stores, or transmits CUI is assessed with the defined frequency.		
RA.L2-3.11.2	a	the frequency to scan for vulnerabilities in organizational systems and applications is defined;		
RA.L2-3.11.2	b	vulnerability scans are performed on organizational systems with the defined frequency;		
RA.L2-3.11.2	c	vulnerability scans are performed on applications with the defined frequency;		

RA.L2-3.11.2	d	vulnerability scans are performed on organizational systems when new vulnerabilities are identified; and		
RA.L2-3.11.2	e	vulnerability scans are performed on applications when new vulnerabilities are identified.		
RA.L2-3.11.3	a	vulnerabilities are identified; and		
RA.L2-3.11.3	b	vulnerabilities are remediated in accordance with risk assessments.		
SC.L1-3.13.1	a	the external system boundary is defined;		
SC.L1-3.13.1	b	key internal system boundaries are defined;		
SC.L1-3.13.1	c	communications are monitored at the external system boundary;		
SC.L1-3.13.1	d	communications are monitored at key internal boundaries;		
SC.L1-3.13.1	e	communications are controlled at the external system boundary;		
SC.L1-3.13.1	f	communications are controlled at key internal boundaries;		
SC.L1-3.13.1	g	communications are protected at the external system boundary; and		
SC.L1-3.13.1	h	communications are protected at key internal boundaries.		
SC.L1-3.13.5	a	publicly accessible system components are identified; and		
SC.L1-3.13.5	b	subnetworks for publicly accessible system components are physically or logically separated from internal networks.		
SC.L2-3.13.10	a	cryptographic keys are established whenever cryptography is employed; and		

SC.L2-3.13.10	b	cryptographic keys are managed whenever cryptography is employed.		
SC.L2-3.13.11	a	FIPS-validated cryptography is employed to protect the confidentiality of CUI.		
SC.L2-3.13.12	a	collaborative computing devices are identified;		
SC.L2-3.13.12	b	collaborative computing devices provide indication to users of devices in use; and		
SC.L2-3.13.12	c	remote activation of collaborative computing devices is prohibited.		
SC.L2-3.13.13	a	use of mobile code is controlled; and		
SC.L2-3.13.13	b	use of mobile code is monitored.		
SC.L2-3.13.14	a	use of Voice over Internet Protocol (VoIP) technologies is controlled; and		
SC.L2-3.13.14	b	use of Voice over Internet Protocol (VoIP) technologies is monitored.		
SC.L2-3.13.15	a	the authenticity of communications sessions is protected.		
SC.L2-3.13.16	a	the confidentiality of CUI at rest is protected.		
SC.L2-3.13.2	a	architectural designs that promote effective information security are identified;		
SC.L2-3.13.2	b	software development techniques that promote effective information security are identified;		
SC.L2-3.13.2	c	systems engineering principles that promote effective information security are identified;		
SC.L2-3.13.2	d	identified architectural designs that promote effective information security are employed;		

SC.L2-3.13.2	e	identified software development techniques that promote effective information security are employed; and		
SC.L2-3.13.2	f	identified systems engineering principles that promote effective information security are employed.		
SC.L2-3.13.3	a	user functionality is identified;		
SC.L2-3.13.3	b	system management functionality is identified; and		
SC.L2-3.13.3	c	user functionality is separated from system management functionality.		
SC.L2-3.13.4	a	unauthorized and unintended information transfer via shared system resources is prevented.		
SC.L2-3.13.6	a	network communications traffic is denied by default; and		
SC.L2-3.13.6	b	network communications traffic is allowed by exception.		
SC.L2-3.13.7	a	remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).		
SC.L2-3.13.8	a	cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified;		
SC.L2-3.13.8	b	alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified; and		
SC.L2-3.13.8	c	either cryptographic mechanisms or alternative physical safeguards are implemented to prevent		

		unauthorized disclosure of CUI during transmission.		
SC.L2-3.13.9	a	a period of inactivity to terminate network connections associated with communications sessions is defined;		
SC.L2-3.13.9	b	network connections associated with communications sessions are terminated at the end of the sessions; and		
SC.L2-3.13.9	c	network connections associated with communications sessions are terminated after the defined period of inactivity.		
SI.L1-3.14.1	a	a time within which to identify system flaws is specified;		
SI.L1-3.14.1	b	system flaws are identified within the specified time frame;		
SI.L1-3.14.1	c	the time within which to report system flaws is specified;		
SI.L1-3.14.1	d	system flaws are reported within the specified time frame;		
SI.L1-3.14.1	e	the time within which to correct system flaws is specified; and		
SI.L1-3.14.1	f	system flaws are corrected within the specified time frame.		
SI.L1-3.14.2	a	designated locations for malicious code protection are identified; and		
SI.L1-3.14.2	b	protection from malicious code at designated locations is provided.		
SI.L1-3.14.4	a	malicious code protection mechanisms are updated when new releases are available.		
SI.L1-3.14.5	a	the frequency for malicious code scans is defined;		

SI.L1-3.14.5	b	malicious code scans are performed with the defined frequency; and		
SI.L1-3.14.5	c	real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.		
SI.L2-3.14.3	a	response actions to system security alerts and advisories are identified;		
SI.L2-3.14.3	b	system security alerts and advisories are monitored; and		
SI.L2-3.14.3	c	actions in response to system security alerts and advisories are taken.		
SI.L2-3.14.6	a	the system is monitored to detect attacks and indicators of potential attacks;		
SI.L2-3.14.6	b	inbound communications traffic is monitored to detect attacks and indicators of potential attacks; and		
SI.L2-3.14.6	c	outbound communications traffic is monitored to detect attacks and indicators of potential attacks.		
SI.L2-3.14.7	a	authorized use of the system is defined; and		
SI.L2-3.14.7	b	unauthorized use of the system is identified.		