CMMC V2.0 – Level 2
System Security Plan (SSP)

<Organization Name>

<Information System Name>

Version <version #>

<version date>

NOTICES

1. CMMC MODEL CONTENT

The CMMC Model is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center and under Contract No. HQ0034-13-D-003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory, LLC, a University Affiliated Research Center.

2. SYSTEM SECURITY PLAN TEMPLATE

System Security Plan

Organization		
	Organization Name	<Organization Name>
	Street Address	<Organization Street Address>
	Suite/Room/Building	<Organization Suite>
	City, State Zip	<Organization City, State Zip>

Document Revision History

Date	Description	Version	Author

TABLE OF CONTENTS

List of Figures

List of Tables

System Security Plan Approvals

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Organization	<Organization Name>		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Organization	<Organization Name>		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Organization	<Organization Name>		

1. Information System

This System Security Plan provides an overview of the security practices and processes for the <Information System Name> (<Information System Abbreviation>) and describes the controls in place or planned for implementation to provide a level of security appropriate for Controlled Unclassified Information (CUI) to be transmitted, processed or stored by the system.
Information security is vital to the Defense Industrial Base and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <Information System Abbreviation> information system.
The security safeguards implemented for the <Information System Abbreviation> system meet the policy and control requirements set forth in this System Security Plan.

1.1. Information System Name/Title

Table 1-1. Information System Name and Title

Information System Name	Information System Abbreviation
<Information System Name>	<Information System Abbreviation>

1.2. System Function

The function and purpose of the <Information System Abbreviation> system is as follows:

<Describe the purpose of the system>

1.3. System Environments of Operation

The following environments are used to develop, test or operate the <Information System Abbreviation> system.

Table 1-2. Environment Name

ENVIRONMENT	
Environment Name	<Environment Name>
Environment Type	<Environment Type>
Operational Description	<Operational Description>

1.4. Network Architecture

The following Network Diagram provides a visual depiction of the system network components that constitute the <Information System Abbreviation> system.

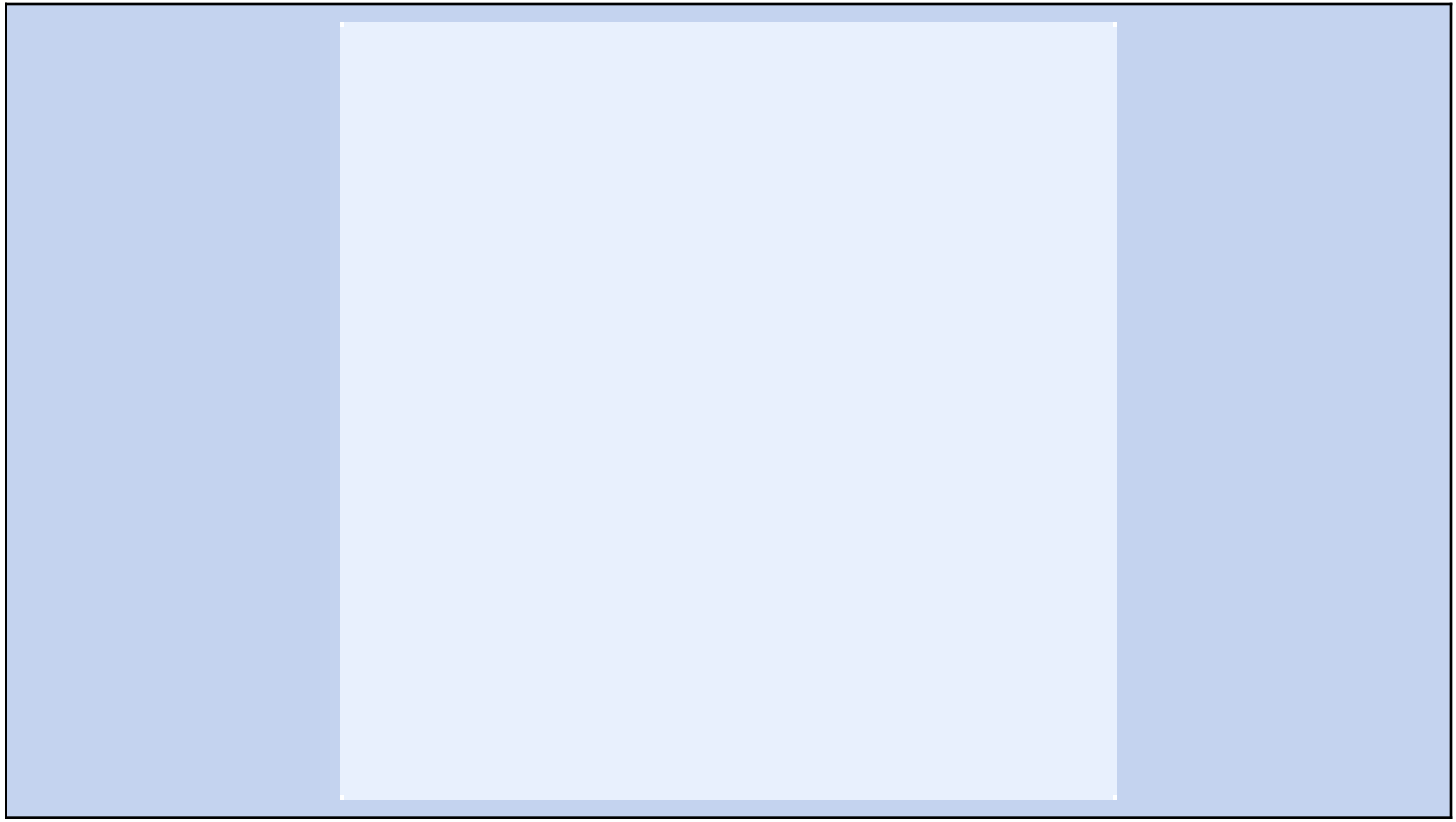

Figure 1-1. Network Diagram

1.5. System Boundary

The following System Boundary Diagram provides a visual depiction of the System Boundary. The boundary separating in-scope components from out-of-scope components is depicted by a prominent border.

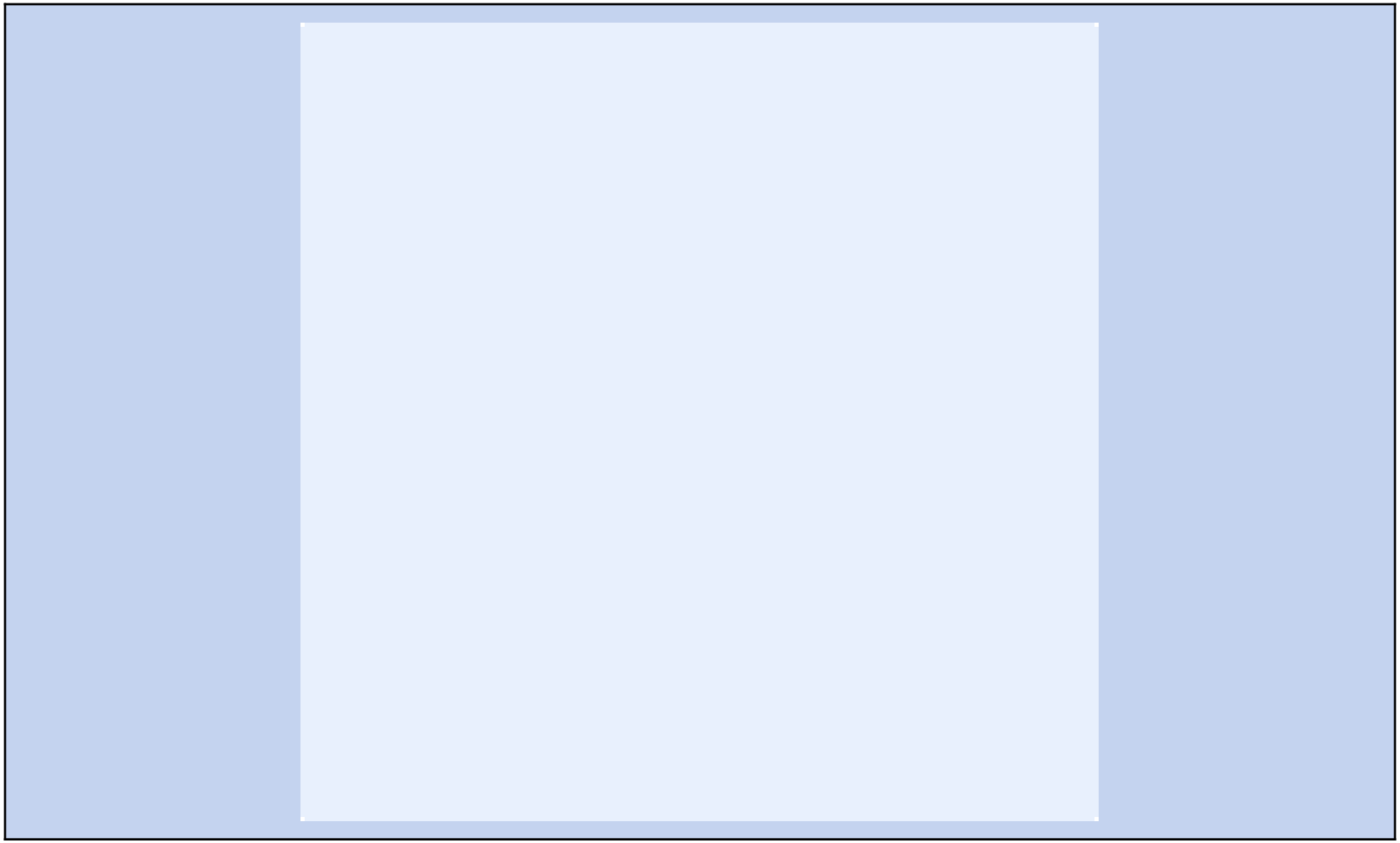

Figure 1-2. System Boundary Diagram

1.6. System Interconnections

Interconnection Name	Description

Table 1-3 - System Interconnections

2. Subjective CMMC Level

<Organization Name> has reviewed the security practices in place for the <Information System Abbreviation> information system and believes this system meets or exceeds the requirements of the following CMMC Level.

Table 2-1. Subjective CMMC Level

CMMC Level
#

3. Organization Contacts

3.1. Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Information System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

3.2. Other Designated Contacts

The following individual(s) possess in-depth knowledge of this system and/or its functions and operation.

Table 3-2. Contact Title

<CONTACT TITLE>	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4. Leveraged Practices and Processes

<Organization Name> may leverage the practices and processes of external organizations or service providers to operate the <Information System Abbreviation> system. External organizations or service providers, if leveraged by <Organization Name>, are identified in the table that follows and referenced throughout this System Security Plan.

Table 4-1. Leveraged External Organizations and Systems

Leveraged Organization/System	Contact Information
<Leveraged Organization/System>	<Leveraged Organization Contact Details>

5. PRACTICES

1.1. ACCESS CONTROL (AC)

AC.L1-3.1.1	Practice Information	Level 1
Reference Name	Authorized Access Control	
Description	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L1-3.1.2	Practice Information	Level 1
Reference Name	Transaction & Function Control	
Description	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.3	Practice Information	Level 2
Reference Name	Control CUI Flow	
Description	Control the flow of CUI in accordance with approved authorizations.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.4	Practice Information	Level 2
Reference Name	Separation of Duties	
Description	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.5	Practice Information	Level 2
Reference Name	Least Privilege	
Description	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.6	Practice Information	Level 2
Reference Name	Non-Privileged Account Use	
Description	Use non-privileged accounts or roles when accessing nonsecurity functions.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.7	Practice Information	Level 2
Reference Name	Privileged Functions	
Description	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.8	Practice Information	Level 2
Reference Name	Unsuccessful Logon Attempts	
Description	Limit unsuccessful logon attempts.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.9	Practice Information	Level 2
Reference Name	Privacy & Security Notices	
Description	Provide privacy and security notices consistent with applicable CUI rules.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.10	Practice Information	Level 2
Reference Name	Session Lock	
Description	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.11	Practice Information	Level 2
Reference Name	Session Termination	
Description	Terminate (automatically) a user session after a defined condition.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.12	Practice Information	Level 2
Reference Name	Control Remote Access	
Description	Monitor and control remote access sessions.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.13	Practice Information	Level 2
Reference Name	Remote Access Confidentiality	
Description	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.14	Practice Information	Level 2
Reference Name	Remote Access Routing	
Description	Route remote access via managed access control points.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.15	Practice Information	Level 2
Reference Name	Privileged Remote Access	
Description	Authorize remote execution of privileged commands and remote access to security-relevant information.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.16	Practice Information	Level 2
Reference Name	Wireless Access Authorization	
Description	Authorize wireless access prior to allowing such connections.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.17	Practice Information	Level 2
Reference Name	Wireless Access Protection	
Description	Protect wireless access using authentication and encryption.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.18	Practice Information	Level 2
Reference Name	Mobile Device Connection	
Description	Control connection of mobile devices.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.19	Practice Information	Level 2
Reference Name	Encrypt CUI on Mobile	
Description	Encrypt CUI on mobile devices and mobile computing platforms.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L1-3.1.20	Practice Information	Level 1
Reference Name	External Connections	
Description	Verify and control/limit connections to and use of external systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L2-3.1.21	Practice Information	Level 2
Reference Name	Portable Storage Use	
Description	Limit use of portable storage devices on external systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AC.L1-3.1.22	Practice Information	Level 1
Reference Name	Control Public Information	
Description	Control information posted or processed on publicly accessible information systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.2. AWARENESS AND TRAINING (AT)

AT.L2-3.2.1	Practice Information	Level 2
Reference Name	Role-Based Risk Awareness	
Description	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.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AT.L2-3.2.2	Practice Information	Level 2
Reference Name	Role-Based Training	
Description	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AT.L2-3.2.3	Practice Information	Level 2
Reference Name	Insider Threat Awareness	
Description	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.3. AUDIT AND ACCOUNTABILITY (AU)

AU.L2-3.3.1	Practice Information	Level 2
Reference Name	System Auditing	
Description	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.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.2	Practice Information	Level 2
Reference Name	User Accountability	
Description	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.3	Practice Information	Level 2
Reference Name	Event Review	
Description	Review and update logged events.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.4	Practice Information	Level 2
Reference Name	Audit Failure Alerting	
Description	Alert in the event of an audit logging process failure.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.5	Practice Information	Level 2
Reference Name	Audit Correlation	
Description	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.6	Practice Information	Level 2
Reference Name	Reduction & Reporting	
Description	Provide audit record reduction and report generation to support on-demand analysis and reporting.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.7	Practice Information	Level 2
Reference Name	Authoritative Time Source	
Description	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.8	Practice Information	Level 2
Reference Name	Audit Protection	
Description	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

AU.L2-3.3.9	Practice Information	Level 2
Reference Name	Audit Management	
Description	Limit management of audit logging functionality to a subset of privileged users.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.4. CONFIGURATION MANAGEMENT (CM)

CM.L2-3.4.1	Practice Information	Level 2
Reference Name	System Baselining	
Description	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.2	Practice Information	Level 2
Reference Name	Security Configuration Enforcement	
Description	Establish and enforce security configuration settings for information technology products employed in organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.3	Practice Information	Level 2
Reference Name	System Change Management	
Description	Track, review, approve or disapprove, and log changes to organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.4	Practice Information	Level 2
Reference Name	Security Impact Analysis	
Description	Analyze the security impact of changes prior to implementation.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.5	Practice Information	Level 2
Reference Name	Access Restrictions for Change	
Description	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.6	Practice Information	Level 2
Reference Name	Least Functionality	
Description	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.7	Practice Information	Level 2
Reference Name	Nonessential Functionality	
Description	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.8	Practice Information	Level 2
Reference Name	Application Execution Policy	
Description	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.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CM.L2-3.4.9	Practice Information	Level 2
Reference Name	User-Installed Software	
Description	Control and monitor user-installed software.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.5. IDENTIFICATION AND AUTHENTICATION (IA)

IA.L1-3.5.1	Practice Information	Level 1
Reference Name	Identification	
Description	Identify information system users, processes acting on behalf of users, and devices.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L1-3.5.2	Practice Information	Level 1
Reference Name	Authentication	
Description	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.3	Practice Information	Level 2
Reference Name	Multifactor Authentication	
Description	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.4	Practice Information	Level 2
Reference Name	Replay-Resistant Authentication	
Description	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.5	Practice Information	Level 2
Reference Name	Identifier Reuse	
Description	Prevent reuse of identifiers for a defined period.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.6	Practice Information	Level 2
Reference Name	Identifier Handling	
Description	Disable identifiers after a defined period of inactivity.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.7	Practice Information	Level 2
Reference Name	Password Complexity	
Description	Enforce a minimum password complexity and change of characters when new passwords are created.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.8	Practice Information	Level 2
Reference Name	Password Reuse	
Description	Prohibit password reuse for a specified number of generations.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.9	Practice Information	Level 2
Reference Name	Temporary Passwords	
Description	Allow temporary password use for system logons with an immediate change to a permanent password.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.10	Practice Information	Level 2
Reference Name	Cryptographically-Protected Passwords	
Description	Store and transmit only cryptographically-protected passwords.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IA.L2-3.5.11	Practice Information	Level 2
Reference Name	Obscure Feedback	
Description	Obscure feedback of authentication information.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.6. INCIDENT RESPONSE (IR)

IR.L2-3.6.1	Practice Information	Level 2
Reference Name	Incident Handling	
Description	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IR.L2-3.6.2	Practice Information	Level 2
Reference Name	Incident Reporting	
Description	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

IR.L2-3.6.3	Practice Information	Level 2
Reference Name	Incident Response Testing	
Description	Test the organizational incident response capability.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.7. MAINTENANCE (MA)

MA.L2-3.7.1	Practice Information	Level 2
Reference Name	Perform Maintenance	
Description	Perform maintenance on organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MA.L2-3.7.2	Practice Information	Level 2
Reference Name	System Maintenance Control	
Description	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MA.L2-3.7.3	Practice Information	Level 2
Reference Name	Equipment Sanitization	
Description	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MA.L2-3.7.4	Practice Information	Level 2
Reference Name	Media Inspection	
Description	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MA.L2-3.7.5	Practice Information	Level 2
Reference Name	Nonlocal Maintenance	
Description	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MA.L2-3.7.6	Practice Information	Level 2
Reference Name	Maintenance Personnel	
Description	Supervise the maintenance activities of maintenance personnel without required access authorization.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.8. MEDIA PROTECTION (MP)

MP.L2-3.8.1	Practice Information	Level 2
Reference Name	Media Protection	
Description	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.2	Practice Information	Level 2
Reference Name	Media Access	
Description	Limit access to CUI on system media to authorized users.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L1-3.8.3	Practice Information	Level 1
Reference Name	Media Disposal	
Description	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.4	Practice Information	Level 2
Reference Name	Media Markings	
Description	Mark media with necessary CUI markings and distribution limitations.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.5	Practice Information	Level 2
Reference Name	Media Accountability	
Description	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.6	Practice Information	Level 2
Reference Name	Portable Storage Encryption	
Description	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.7	Practice Information	Level 2
Reference Name	Removable Media	
Description	Control the use of removable media on system components.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.8	Practice Information	Level 2
Reference Name	Shared Media	
Description	Prohibit the use of portable storage devices when such devices have no identifiable owner.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

MP.L2-3.8.9	Practice Information	Level 2
Reference Name	Protect Backups	
Description	Protect the confidentiality of backup CUI at storage locations.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.9. PERSONNEL SECURITY (PS)

PS.L2-3.9.1	Practice Information	Level 2
Reference Name	Screen Individuals	
Description	Screen individuals prior to authorizing access to organizational systems containing CUI.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PS.L2-3.9.2	Practice Information	Level 2
Reference Name	Personnel Actions	
Description	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.10. PHYSICAL PROTECTION (PE)

PE.L1-3.10.1	Practice Information	Level 1
Reference Name	Limit Physical Access	
Description	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PE.L2-3.10.2	Practice Information	Level 2
Reference Name	Monitor Facility	
Description	Protect and monitor the physical facility and support infrastructure for organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PE.L1-3.10.3	Practice Information	Level 1
Reference Name	Escort Visitors	
Description	Escort visitors and monitor visitor activity.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PE.L1-3.10.4	Practice Information	Level 1
Reference Name	Physical Access Logs	
Description	Maintain audit logs of physical access.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PE.L1-3.10.5	Practice Information	Level 1
Reference Name	Manage Physical Access	
Description	Control and manage physical access devices.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

PE.L2-3.10.6	Practice Information	Level 2
Reference Name	Alternative Work Sites	
Description	Enforce safeguarding measures for CUI at alternate work sites.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

I.11. RISK ASSESSMENT (RA)

RA.L2-3.11.1	Practice Information	Level 2
Reference Name	Risk Assessments	
Description	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.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

RA.L2-3.11.2	Practice Information	Level 2
Reference Name	Vulnerability Scan	
Description	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

RA.L2-3.11.3	Practice Information	Level 2
Reference Name	Vulnerability Remediation	
Description	Remediate vulnerabilities in accordance with risk assessments.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.12. SECURITY ASSESSMENT (CA)

CA.L2-3.12.1	Practice Information	Level 2
Reference Name	Security Control Assessment	
Description	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CA.L2-3.12.2	Practice Information	Level 2
Reference Name	Plan of Action	
Description	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CA.L2-3.12.3	Practice Information	Level 2
Reference Name	Security Control Monitoring	
Description	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

CA.L2-3.12.4	Practice Information	Level 2
Reference Name	System Security Plan	
Description	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.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.13. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

SC.L1-3.13.1	Practice Information	Level 1
Reference Name	Boundary Protection	
Description	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 organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.2	Practice Information	Level 2
Reference Name	Security Engineering	
Description	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.3	Practice Information	Level 2
Reference Name	Role Separation	
Description	Separate user functionality from system management functionality.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.4	Practice Information	Level 2
Reference Name	Shared Resource Control	
Description	Prevent unauthorized and unintended information transfer via shared system resources.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L1-3.13.5	Practice Information	Level 1
Reference Name	Public-Access System Separation	
Description	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.6	Practice Information	Level 2
Reference Name	Network Communication by Exception	
Description	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.7	Practice Information	Level 2
Reference Name	Split Tunneling	
Description	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).	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.8	Practice Information	Level 2
Reference Name	Data in Transit	
Description	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.9	Practice Information	Level 2
Reference Name	Connections Termination	
Description	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.10	Practice Information	Level 2
Reference Name	Key Management	
Description	Establish and manage cryptographic keys for cryptography employed in organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.11	Practice Information	Level 2
Reference Name	CUI Encryption	
Description	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.12	Practice Information	Level 2
Reference Name	Collaborative Device Control	
Description	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.13	Practice Information	Level 2
Reference Name	Mobile Code	
Description	Control and monitor the use of mobile code.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.14	Practice Information	Level 2
Reference Name	Voice over Internet Protocol	
Description	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.15	Practice Information	Level 2
Reference Name	Communications Authenticity	
Description	Protect the authenticity of communications sessions.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SC.L2-3.13.16	Practice Information	Level 2
Reference Name	Data at Rest	
Description	Protect the confidentiality of CUI at rest.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

1.14. SYSTEM AND INFORMATION INTEGRITY (SI)

SI.L1-3.14.1	Practice Information	Level 1
Reference Name	Flaw Remediation	
Description	Identify, report, and correct information and information system flaws in a timely manner.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L1-3.14.2	Practice Information	Level 1
Reference Name	Malicious Code Protection	
Description	Provide protection from malicious code at appropriate locations within organizational information systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L2-3.14.3	Practice Information	Level 2
Reference Name	Security Alerts & Advisories	
Description	Monitor system security alerts and advisories and take action in response.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L1-3.14.4	Practice Information	Level 1
Reference Name	Update Malicious Code Protection	
Description	Update malicious code protection mechanisms when new releases are available.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L1-3.14.5	Practice Information	Level 1
Reference Name	System & File Scanning	
Description	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L2-3.14.6	Practice Information	Level 2
Reference Name	Monitor Communications for Attacks	
Statement	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

SI.L2-3.14.7	Practice Information	Level 2
Reference Name	Identify Unauthorized Use	
Statement	Identify unauthorized use of organizational systems.	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Not applicable □ Inherited: □ Not Implemented		
Implementation Details:		

Appendix A – CMMC POA&M Template

Plan of Action and Milestones (POA&M)				
POA&M ID		Date Created	Click or tap to enter a date.	
Practice ID		Point of Contact		
Deficiency Title		POA&M Status	Choose an item.	
Deficiency Description				
Milestone #1	Scheduled Completion Date	Click or tap to enter a date.	Milestone Status	Choose an item.
	Planned Milestone			
	Actions Taken			
Milestone #2	Scheduled Completion Date	Click or tap to enter a date.	Milestone Status	Choose an item.
	Planned Milestone			
	Actions Taken			
Milestone #3	Scheduled Completion Date	Click or tap to enter a date.	Milestone Status	Choose an item.

Plan of Action and Milestones (POA&M)		
	Planned Milestone	
	Actions Taken	

