Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
AC	**Authorized Access Control**	**L1**	**AC.L1-3.1.1**		**Limit information system access to authorized users, processes acting on behalf of authorized users or devices [including other information systems].**			
AC	Authorized Access Control	L1		AC.L1-3.1.1[a]	authorized users are identified.	x	x	OSC provides the information for the user account and we enter it / user form
AC	Authorized Access Control	L1		AC.L1-3.1.1[b]	processes acting on behalf of authorized users are identified.	x		
AC	Authorized Access Control	L1		AC.L1-3.1.1[c]	devices (and other systems) authorized to connect to the system are identified.	x		
AC	Authorized Access Control	L1		AC.L1-3.1.1[d]	system access is limited to authorized users.	x		
AC	Authorized Access Control	L1		AC.L1-3.1.1[e]	system access is limited to processes acting on behalf of authorized users.	x		
AC	Authorized Access Control	L1		AC.L1-3.1.1[f]	system access is limited to authorized devices (including other systems).	x		
AC	**Transaction & Function Control**	**L1**	**AC.L1-3.1.2**		**Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**			
AC	Transaction & Function Control	L1		AC.L1-3.1.2[a]	the types of transactions and functions that authorized users are permitted to execute are defined.	x	x	
AC	Transaction & Function Control	L1		AC.L1-3.1.2[b]	system access is limited to the defined types of transactions and functions for authorized users.	x	x	
AC	**Control CUI Flow**	**L2**	**AC.L2-3.1.3**		**Control the flow of CUI in accordance with approved authorizations.**			
AC	Control CUI Flow	L2		AC.L2-3.1.3[a]	information flow control policies are defined.	x		
AC	Control CUI Flow	L2		AC.L2-3.1.3[b]	methods and enforcement mechanisms for controlling the flow of CUI are defined.	x		
AC	Control CUI Flow	L2		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.	x		
AC	Control CUI Flow	L2		AC.L2-3.1.3[d]	authorizations for controlling the flow of CUI are defined.	x		
AC	Control CUI Flow	L2		AC.L2-3.1.3[e]	approved authorizations for controlling the flow of CUI are enforced.			Selection of individuals is the clients responsibility. Implimenting the clients approvals is ITG re
AC	**Separation of Duties**	**L2**	**AC.L2-3.1.4**		**Separate the duties of individuals to reduce the risk of malevolent activity without collusion.**			
AC	Separation of Duties	L2		AC.L2-3.1.4[a]	the duties of individuals requiring separation are defined.	x		
AC	Separation of Duties	L2		AC.L2-3.1.4[b]	responsibilities for duties that require separation are assigned to separate individuals.	x		
AC	Separation of Duties	L2		AC.L2-3.1.4[c]	access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.	x		
AC	**Least Privilege**	**L2**	**AC.L2-3.1.5**		**Employ the principle of least privilege, including for specific security functions and privileged accounts.**			
AC	Least Privilege	L2		AC.L2-3.1.5[a]	privileged accounts are identified.	x		
AC	Least Privilege	L2		AC.L2-3.1.5[b]	access to privileged accounts is authorized in accordance with the principle of least privilege.	x		
AC	Least Privilege	L2		AC.L2-3.1.5[c]	security functions are identified.	x		
AC	Least Privilege	L2		AC.L2-3.1.5[d]	access to security functions is authorized in accordance with the principle of least privilege.	x		
AC	**Non-Privileged Account Use**	**L2**	**AC.L2-3.1.6**		**Use non-privileged accounts or roles when accessing nonsecurity functions.**			
AC	Non-Privileged Account Use	L2		AC.L2-3.1.6[a]	nonsecurity functions are identified.	x		
AC	Non-Privileged Account Use	L2		AC.L2-3.1.6[b]	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.	x		
AC	**Privileged Functions**	**L2**	**AC.L2-3.1.7**		**Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.**			
AC	Privileged Functions	L2		AC.L2-3.1.7[a]	privileged functions are defined.	x		
AC	Privileged Functions	L2		AC.L2-3.1.7[b]	non-privileged users are defined.	x		
AC	Privileged Functions	L2		AC.L2-3.1.7[c]	non-privileged users are prevented from executing privileged functions.	x		
AC	Privileged Functions	L2		AC.L2-3.1.7[d]	the execution of privileged functions is captured in audit logs.	x		
AC	**Unsuccessful Logon Attempts**	**L2**	**AC.L2-3.1.8**		**Limit unsuccessful logon attempts.**			
AC	Unsuccessful Logon Attempts	L2		AC.L2-3.1.8[a]	the means of limiting unsuccessful logon attempts is defined.	x		
AC	Unsuccessful Logon Attempts	L2		AC.L2-3.1.8[b]	the defined means of limiting unsuccessful logon attempts is implemented.	x		
AC	**Privacy & Security Notices**	**L2**	**AC.L2-3.1.9**		**Provide privacy and security notices consistent with applicable Controlled Unclassified Information [CUI] rules.**			
AC	Privacy & Security Notices	L2		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.	x		
AC	Privacy & Security Notices	L2		AC.L2-3.1.9[b]	privacy and security notices are displayed.	x		
AC	**Session Lock**	**L2**	**AC.L2-3.1.10**		**Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.**			
AC	Session Lock	L2		AC.L2-3.1.10[a]	the period of inactivity after which the system initiates a session lock is defined.	x		
AC	Session Lock	L2		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.	x		
AC	Session Lock	L2		AC.L2-3.1.10[c]	previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.	x		
AC	**Session Termination**	**L2**	**AC.L2-3.1.11**		**Terminate [automatically] user sessions after a defined condition.**			
AC	Session Termination	L2		AC.L2-3.1.11[a]	conditions requiring a user session to terminate are defined.	x		
AC	Session Termination	L2		AC.L2-3.1.11[b]	a user session is automatically terminated after any of the defined conditions occur.	x		
AC	**Control Remote Access**	**L2**	**AC.L2-3.1.12**		**Monitor and control remote access sessions.**			
AC	Control Remote Access	L2		AC.L2-3.1.12[a]	remote access sessions are permitted.	x		
AC	Control Remote Access	L2		AC.L2-3.1.12[b]	the types of permitted remote access are identified.	x		
AC	Control Remote Access	L2		AC.L2-3.1.12[c]	remote access sessions are controlled.	x		
AC	Control Remote Access	L2		AC.L2-3.1.12[d]	remote access sessions are monitored.	x		
AC	**Remote Access Confidentiality**	**L2**	**AC.L2-3.1.13**		**Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.**			
AC	Remote Access Confidentiality	L2		AC.L2-3.1.13[a]	cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.	x		
AC	Remote Access Confidentiality	L2		AC.L2-3.1.13[b]	cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.	x		
AC	**Remote Access Routing**	**L2**	**AC.L2-3.1.14**		**Route remote access via managed access control points.**			
AC	Remote Access Routing	L2		AC.L2-3.1.14[a]	managed access control points are identified and implemented.	x		
AC	Remote Access Routing	L2		AC.L2-3.1.14[b]	remote access is routed through managed network access control points.	x		
AC	**Privileged Remote Access**	**L2**	**AC.L2-3.1.15**		**Authorize remote execution of privileged commands and remote access to security-relevant information.**			
AC	Privileged Remote Access	L2		AC.L2-3.1.15[a]	privileged commands authorized for remote execution are identified.	x		
AC	Privileged Remote Access	L2		AC.L2-3.1.15[b]	security-relevant information authorized to be accessed remotely is identified.	x		
AC	Privileged Remote Access	L2		AC.L2-3.1.15[c]	the execution of the identified privileged commands via remote access is authorized.	x		
AC	Privileged Remote Access	L2		AC.L2-3.1.15[d]	access to the identified security-relevant information via remote access is authorized.	x		
AC	**Wireless Access Authorization**	**L2**	**AC.L2-3.1.16**		**Authorize wireless access prior to allowing such connections.**			
AC	Wireless Access Authorization	L2		AC.L2-3.1.16[a]	wireless access points are identified.	n/a		
AC	Wireless Access Authorization	L2		AC.L2-3.1.16[b]	wireless access is authorized prior to allowing such connections.	n/a		
AC	**Wireless Access Protection**	**L2**	**AC.L2-3.1.17**		**Protect wireless access using authentication and encryption.**			
AC	Wireless Access Protection	L2		AC.L2-3.1.17[a]	wireless access to the system is protected using authentication.	n/a		
AC	Wireless Access Protection	L2		AC.L2-3.1.17[b]	wireless access to the system is protected using encryption.	n/a		
AC	**Mobile Device Connection**	**L2**	**AC.L2-3.1.18**		**Control connection of mobile devices.**			
AC	Mobile Device Connection	L2		AC.L2-3.1.18[a]	mobile devices that process, store, or transmit CUI are identified.	n/a		

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
AC	Mobile Device Connection	L2		AC.L2-3.1.18[b]	mobile device connections are authorized.	n//a		
AC	Mobile Device Connection	L2		AC.L2-3.1.18[c]	mobile device connections are monitored and logged.	n//a		
AC	**Encrypt CUI on Mobile**	**L2**	**AC.L2-3.1.19**		**Encrypt CUI on mobile devices and mobile computing platforms.**			
AC	Encrypt CUI on Mobile	L2		AC.L2-3.1.19[a]	mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.	n/a		
AC	Encrypt CUI on Mobile	L2		AC.L2-3.1.19[b]	encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.	n/a		
AC	**External Connections**	**L1**	**AC.L1-3.1.20**		**Verify and control/limit connections to and use of external information systems.**			
AC	External Connections	L1		AC.L1-3.1.20[a]	connections to external systems are identified.	x		
AC	External Connections	L1		AC.L1-3.1.20[b]	the use of external systems is identified.	x		
AC	External Connections	L1		AC.L1-3.1.20[c]	connections to external systems are verified.	x		
AC	External Connections	L1		AC.L1-3.1.20[d]	the use of external systems is verified.	x		
AC	External Connections	L1		AC.L1-3.1.20[e]	connections to external systems are controlled/limited.	x		
AC	External Connections	L1		AC.L1-3.1.20[f]	the use of external systems is controlled/limited.	x		
AC	**Portable Storage Use**	**L2**	**AC.L2-3.1.21**		**Limit use of portable storage devices on external systems.**			
AC	Portable Storage Use	L2		AC.L2-3.1.21[a]	the use of portable storage devices containing CUI on external systems is identified and documented.	x		
AC	Portable Storage Use	L2		AC.L2-3.1.21[b]	limits on the use of portable storage devices containing CUI on external systems are defined.	x		
AC	Portable Storage Use	L2		AC.L2-3.1.21[c]	the use of portable storage devices containing CUI on external systems is limited as defined.	x		
AC	**Control Public Information**	**L1**	**AC.L1-3.1.22**		**Control information posted or processed on publicly accessible information systems.**			
AC	Control Public Information	L1		AC.L1-3.1.22[a]	individuals authorized to post or process information on publicly accessible systems are identified.		x	
AC	Control Public Information	L1		AC.L1-3.1.22[b]	procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.		x	
AC	Control Public Information	L1		AC.L1-3.1.22[c]	a review process is in place prior to posting of any content to publicly accessible systems.		x	
AC	Control Public Information	L1		AC.L1-3.1.22[d]	content on publicly accessible systems is reviewed to ensure that it does not include CUI.		x	
AC	Control Public Information	L1		AC.L1-3.1.22[e]	mechanisms are in place to remove and address improper posting of CUI.		x	
AT	**Role-Based Risk Awareness**	**L2**	**AT.L2-3.2.1**		**Ensure that managers, system 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.**			
AT	Role-Based Risk Awareness	L2		AT.L2-3.2.1[a]	security risks associated with organizational activities involving CUI are identified.	x	x	
AT	Role-Based Risk Awareness	L2		AT.L2-3.2.1[b]	policies, standards, and procedures related to the security of the system are identified.	x	x	
AT	Role-Based Risk Awareness	L2		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.	x	x	
AT	Role-Based Risk Awareness	L2		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.	x	x	
AT	**Role-Based Training**	**L2**	**AT.L2-3.2.2**		**Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.**			
AT	Role-Based Training	L2		AT.L2-3.2.2[a]	information security-related duties, roles, and responsibilities are defined.	x	x	
AT	Role-Based Training	L2		AT.L2-3.2.2[b]	information security-related duties, roles, and responsibilities are assigned to designated personnel.	x	x	ITG will write policies / OSC will implement within own organization
AT	Role-Based Training	L2		AT.L2-3.2.2[c]	personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.	x	x	
AT	**Insider Threat Awareness**	**L2**	**AT.L2-3.2.3**		**Provide security awareness training on recognizing and reporting potential indicators of insider threat.**			
AT	Insider Threat Awareness	L2		AT.L2-3.2.3[a]	potential indicators associated with insider threats are identified.	x	x	
AT	Insider Threat Awareness	L2		AT.L2-3.2.3[b]	security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.	x	x	
AU	**System Auditing**	**L2**	**AU.L2-3.3.1**		**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.**			
AU	System Auditing	L2		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.	x		
AU	System Auditing	L2		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.	x		
AU	System Auditing	L2		AU.L2-3.3.1[c]	audit records are created (generated).	x		
AU	System Auditing	L2		AU.L2-3.3.1[d]	audit records, once created, contain the defined content.	x		
AU	System Auditing	L2		AU.L2-3.3.1[e]	retention requirements for audit records are defined.	x		
AU	System Auditing	L2		AU.L2-3.3.1[f]	audit records are retained as defined.	x		
AU	**User Accountability**	**L2**	**AU.L2-3.3.2**		**Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.**			
AU	User Accountability	L2		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.	x		
AU	User Accountability	L2		AU.L2-3.3.2[b]	audit records, once created, contain the defined content.	x		
AU	**Event Review**	**L2**	**AU.L2-3.3.3**		**Review and update logged events.**			
AU	Event Review	L2		AU.L2-3.3.3[a]	a process for determining when to review logged events is defined.	x		
AU	Event Review	L2		AU.L2-3.3.3[b]	event types being logged are reviewed in accordance with the defined review process.	x		
AU	Event Review	L2		AU.L2-3.3.3[c]	event types being logged are updated based on the review.	x		
AU	**Audit Failure Alerting**	**L2**	**AU.L2-3.3.4**		**Alert in the event of an audit logging process failure.**			
AU	Audit Failure Alerting	L2		AU.L2-3.3.4[a]	personnel or roles to be alerted in the event of an audit logging process failure are identified.	x		
AU	Audit Failure Alerting	L2		AU.L2-3.3.4[b]	types of audit logging process failures for which alert will be generated are defined.	x		
AU	Audit Failure Alerting	L2		AU.L2-3.3.4[c]	identified personnel or roles are alerted in the event of an audit logging process failure.	x		
AU	**Audit Correlation**	**L2**	**AU.L2-3.3.5**		**Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.**			
AU	Audit Correlation	L2		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.	x	x	
AU	Audit Correlation	L2		AU.L2-3.3.5[b]	defined audit record review, analysis, and reporting processes are correlated.	x	x	
AU	**Reduction & Reporting**	**L2**	**AU.L2-3.3.6**		**Provide audit record reduction and report generation to support on-demand analysis and reporting.**			

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
AU	Reduction & Reporting	L2		AU.L2-3.3.6[a]	an audit record reduction capability that supports on-demand analysis is provided.	x		
AU	Reduction & Reporting	L2		AU.L2-3.3.6[b]	a report generation capability that supports on-demand reporting is provided.	x		
AU	**Authoritative Time Source**	**L2**	**AU.L2-3.3.7**		**Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.**			
AU	Authoritative Time Source	L2		AU.L2-3.3.7[a]	internal system clocks are used to generate time stamps for audit records.	x		
AU	Authoritative Time Source	L2		AU.L2-3.3.7[b]	an authoritative source with which to compare and synchronize internal system clocks is specified.	x		
AU	Authoritative Time Source	L2		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.	x		
AU	**Audit Protection**	**L2**	**AU.L2-3.3.8**		**Protect audit information and audit logging tools from unauthorized access, modification and deletion.**			
AU	Audit Protection	L2		AU.L2-3.3.8[a]	audit information is protected from unauthorized access.	x		
AU	Audit Protection	L2		AU.L2-3.3.8[b]	audit information is protected from unauthorized modification.	x		
AU	Audit Protection	L2		AU.L2-3.3.8[c]	audit information is protected from unauthorized deletion.	x		
AU	Audit Protection	L2		AU.L2-3.3.8[d]	audit logging tools are protected from unauthorized access.	x		
AU	Audit Protection	L2		AU.L2-3.3.8[e]	audit logging tools are protected from unauthorized modification.	x		
AU	Audit Protection	L2		AU.L2-3.3.8[f]	audit logging tools are protected from unauthorized deletion.	x		
AU	**Audit Management**	**L2**	**AU.L2-3.3.9**	**AU.L2-3.3.9**	**Limit management of audit logging functionality to a subset of privileged users.**			
AU	Audit Management	L2		AU.L2-3.3.9[a]	a subset of privileged users granted access to manage audit logging functionality is defined.	x		
AU	Audit Management	L2		AU.L2-3.3.9[b]	management of audit logging functionality is limited to the defined subset of privileged users.	x		
CM	**System Baselining**	**L2**	**CM.L2-3.4.1**		**Establish and maintain baseline configurations and inventories of organizational systems [including hardware, software, firmware and documentation] throughout the respective system development life cycles.**			
CM	System Baselining	L2		CM.L2-3.4.1[a]	a baseline configuration is established.	x		
CM	System Baselining	L2		CM.L2-3.4.1[b]	the baseline configuration includes hardware, software, firmware, and documentation.	x		
CM	System Baselining	L2		CM.L2-3.4.1[c]	the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.	x		
CM	System Baselining	L2		CM.L2-3.4.1[d]	a system inventory is established.	x		
CM	System Baselining	L2		CM.L2-3.4.1[e]	the system inventory includes hardware, software, firmware, and documentation.	x		
CM	System Baselining	L2		CM.L2-3.4.1[f]	the inventory is maintained (reviewed and updated) throughout the system development life cycle.	x		
CM	**Security Configuration Enforcement**	**L2**	**CM.L2-3.4.2**		**Establish and enforce security configuration settings for information technology products employed in organizational systems.**			
CM	Security Configuration Enforcement	L2		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.	x		
CM	Security Configuration Enforcement	L2		CM.L2-3.4.2[b]	security configuration settings for information technology products employed in the system are enforced.	x		
CM	**System Change Management**	**L2**	**CM.L2-3.4.3**		**Track, review, approve or disapprove and log changes to organizational systems.**			
CM	System Change Management	L2		CM.L2-3.4.3[a]	changes to the system are tracked.	x		
CM	System Change Management	L2		CM.L2-3.4.3[b]	changes to the system are reviewed.	x		
CM	System Change Management	L2		CM.L2-3.4.3[c]	changes to the system are approved or disapproved.	x	x	ITG will record CRs, client will approve or dis approve CRs ,itg will implement CRs
CM	System Change Management	L2		CM.L2-3.4.3[d]	changes to the system are logged.	x		
CM	**Security Impact Analysis**	**L2**	**CM.L2-3.4.4**		**Analyze the security impact of changes prior to implementation.**			
CM	Security Impact Analysis	L2		CM.L2-3.4.4	the security impact of changes to the system is analyzed prior to implementation.	x		
CM	**Access Restrictions for Change**	**L2**	**CM.L2-3.4.5**		**Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.**			
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[a]	physical access restrictions associated with changes to the system are defined.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[b]	physical access restrictions associated with changes to the system are documented.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[c]	physical access restrictions associated with changes to the system are approved.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[d]	physical access restrictions associated with changes to the system are enforced.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[e]	logical access restrictions associated with changes to the system are defined.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[f]	logical access restrictions associated with changes to the system are documented.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[g]	logical access restrictions associated with changes to the system are approved.	x		
CM	Access Restrictions for Change	L2		CM.L2-3.4.5[h]	logical access restrictions associated with changes to the system are enforced.	x		
CM	**Least Functionality**	**L2**	**CM.L2-3.4.6**		**Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.**			
CM	Least Functionality	L2		CM.L2-3.4.6[a]	essential system capabilities are defined based on the principle of least functionality.	x		
CM	Least Functionality	L2		CM.L2-3.4.6[b]	the system is configured to provide only the defined essential capabilities.	x		
CM	**Nonessential Functionality**	**L2**	**CM.L2-3.4.7**		**Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.**			
CM	Nonessential Functionality	L2		CM.L2-3.4.7[a]	essential programs are defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[b]	the use of nonessential programs is defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[c]	the use of nonessential programs is restricted, disabled, or prevented as defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[d]	essential functions are defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[e]	the use of nonessential functions is defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[f]	the use of nonessential functions is restricted, disabled, or prevented as defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[g]	essential ports are defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[h]	the use of nonessential ports is defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[i]	the use of nonessential ports is restricted, disabled, or prevented as defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[j]	essential protocols are defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[k]	the use of nonessential protocols is defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[l]	the use of nonessential protocols is restricted, disabled, or prevented as defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[m]	essential services are defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[n]	the use of nonessential services is defined.	x		
CM	Nonessential Functionality	L2		CM.L2-3.4.7[o]	the use of nonessential services is restricted, disabled, or prevented as defined.	x		
CM	**Application Execution Policy**	**L2**	**CM.L2-3.4.8**		**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.**			
CM	Application Execution Policy	L2		CM.L2-3.4.8[a]	a policy specifying whether whitelisting or blacklisting is to be implemented is specified.	x		

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
CM	Application Execution Policy	L2		CM.L2-3.4.8[b]	the software allowed to execute under whitelisting or denied use under blacklisting is specified.	x		
CM	Application Execution Policy	L2		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.	x		
CM	**User-Installed Software**	**L2**	**CM.L2-3.4.9**		**Control and monitor user-installed software.**			
CM	User-Installed Software	L2		CM.L2-3.4.9[a]	a policy for controlling the installation of software by users is established.	x		
CM	User-Installed Software	L2		CM.L2-3.4.9[b]	installation of software by users is controlled based on the established policy.	x		
CM	User-Installed Software	L2		CM.L2-3.4.9[c]	installation of software by users is monitored.	x		
IA	**Identification**	**L1**	**IA.L1-3.5.1**		**Identify information system users, processes acting on behalf of users or devices.**			
IA	Identification	L1		IA.L1-3.5.1[a]	system users are identified.	x		
IA	Identification	L1		IA.L1-3.5.1[b]	processes acting on behalf of users are identified.	x		
IA	Identification	L1		IA.L1-3.5.1[c]	devices accessing the system are identified.	x		
IA	**Authentication**	**L1**	**IA.L1-3.5.2**		**Authenticate [or verify] the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.**			
IA	Authentication	L1		IA.L1-3.5.2[a]	the identity of each user is authenticated or verified as a prerequisite to system access.	x		
IA	Authentication	L1		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.	x		
IA	Authentication	L1		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.	x		
IA	**Multifactor Authentication**	**L2**	**IA.L2-3.5.3**		**Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.**			
IA	Multifactor Authentication	L2		IA.L2-3.5.3[a]	privileged accounts are identified.	x		
IA	Multifactor Authentication	L2		IA.L2-3.5.3[b]	multifactor authentication is implemented for local access to privileged accounts.	x		
IA	Multifactor Authentication	L2		IA.L2-3.5.3[c]	multifactor authentication is implemented for network access to privileged accounts.	x		
IA	Multifactor Authentication	L2		IA.L2-3.5.3[d]	multifactor authentication is implemented for network access to non-privileged accounts.	x		
IA	**Replay-Resistant Authentication**	**L2**	**IA.L2-3.5.4**		**Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.**			
IA	Replay-Resistant Authentication	L2		IA.L2-3.5.4	replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.	x		
IA	**Identifier Reuse**	**L2**	**IA.L2-3.5.5**	**IA.L2-3.5.5**	**Prevent the reuse of identifiers for a defined period.**			
IA	Identifier Reuse	L2		IA.L2-3.5.5[a]	a period within which identifiers cannot be reused is defined.	x		
IA	Identifier Reuse	L2		IA.L2-3.5.5[b]	reuse of identifiers is prevented within the defined period.	x		
IA	**Identifier Handling**	**L2**	**IA.L2-3.5.6**		**Disable identifiers after a defined period of inactivity.**			
IA	Identifier Handling	L2		IA.L2-3.5.6[a]	a period of inactivity after which an identifier is disabled is defined.	x		
IA	Identifier Handling	L2		IA.L2-3.5.6[b]	identifiers are disabled after the defined period of inactivity.	x		
IA	**Password Complexity**	**L2**	**IA.L2-3.5.7**		**Enforce a minimum password complexity and change of characters when new passwords are created.**			
IA	Password Complexity	L2		IA.L2-3.5.7[a]	password complexity requirements are defined.	x		
IA	Password Complexity	L2		IA.L2-3.5.7[b]	password change of character requirements are defined.	x		
IA	Password Complexity	L2		IA.L2-3.5.7[c]	minimum password complexity requirements as defined are enforced when new passwords are created.	x		
IA	Password Complexity	L2		IA.L2-3.5.7[d]	minimum password change of character requirements as defined are enforced when new passwords are created.	x		
IA	**Password Reuse**	**L2**	**IA.L2-3.5.8**		**Prohibit password reuse for a specified number of generations.**			
IA	Password Reuse	L2		IA.L2-3.5.8[a]	the number of generations during which a password cannot be reused is specified.	x		
IA	Password Reuse	L2		IA.L2-3.5.8[b]	reuse of passwords is prohibited during the specified number of generations.	x		
IA	**Temporary Passwords**	**L2**	**IA.L2-3.5.9**		**Allow temporary password use for system logons with an immediate change to a permanent password.**			
IA	Temporary Passwords	L2		IA.L2-3.5.9	an immediate change to a permanent password is required when a temporary password is used for system logon.	x	x	User must change the system provided password
IA	**Cryptographically-Protected Passwords**	**L2**	**IA.L2-3.5.10**		**Store and transmit only cryptographically- protected passwords.**			
IA	Cryptographically-Protected Passwords	L2		IA.L2-3.5.10[a]	passwords are cryptographically protected in storage.	x		
IA	Cryptographically-Protected Passwords	L2		IA.L2-3.5.10[b]	passwords are cryptographically protected in transit.	x		
IA	**Obscure Feedback**	**L2**	**IA.L2-3.5.11**		**Obscure feedback of authentication information.**			
IA	Obscure Feedback	L2		IA.L2-3.5.11	authentication information is obscured during the authentication process.	x		
IR	**Incident Handling**	**L2**	**IR.L2-3.6.1**		**Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.**			
IR	Incident Handling	L2		IR.L2-3.6.1[a]	an operational incident-handling capability is established.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[b]	the operational incident-handling capability includes preparation.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[c]	the operational incident-handling capability includes detection.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[d]	the operational incident-handling capability includes analysis.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[e]	the operational incident-handling capability includes containment.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[f]	the operational incident-handling capability includes recovery.	x		
IR	Incident Handling	L2		IR.L2-3.6.1[g]	the operational incident-handling capability includes user response activities.	x		
IR	**Incident Reporting**	**L2**	**IR.L2-3.6.2**		**Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.**			in the event that incidents are brought to the attention of OSC's user community they must be reported to ITG for further in
IR	Incident Reporting	L2		IR.L2-3.6.2[a]	incidents are tracked.	x		
IR	Incident Reporting	L2		IR.L2-3.6.2[b]	incidents are documented.	x		
IR	Incident Reporting	L2		IR.L2-3.6.2[c]	authorities to whom incidents are to be reported are identified.	x		
IR	Incident Reporting	L2		IR.L2-3.6.2[d]	organizational officials to whom incidents are to be reported are identified.	x		OSC will have to provide an organizational chart of CMMC related of.
IR	Incident Reporting	L2		IR.L2-3.6.2[e]	identified authorities are notified of incidents.	x		
IR	Incident Reporting	L2		IR.L2-3.6.2[f]	identified organizational officials are notified of incidents.	x		
IR	**Incident Response Testing**	**L2**	**IR.L2-3.6.3**		**Test the organizational incident response capability.**			
IR	Incident Response Testing	L2		IR.L2-3.6.3	Determine if, for an organizational system that processes, stores, or transmits CUI, the incident response capability is tested.	x	x	desktop ex. Will be performed by OCS and ITG
MA	**Perform Maintenance**	**L2**	**MA.L2-3.7.1**		**Perform maintenance on organizational systems.**			
MA	Perform Maintenance	L2		MA.L2-3.7.1	system maintenance is performed.	x		
MA	**System Maintenance Control**	**L2**	**MA.L2-3.7.2**		**Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.**			
MA	System Maintenance Control	L2		MA.L2-3.7.2[a]	tools used to conduct system maintenance are controlled.	x		
MA	System Maintenance Control	L2		MA.L2-3.7.2[b]	techniques used to conduct system maintenance are controlled.	x		
MA	System Maintenance Control	L2		MA.L2-3.7.2[c]	mechanisms used to conduct system maintenance are controlled.	x		
MA	System Maintenance Control	L2		MA.L2-3.7.2[d]	personnel used to conduct system maintenance are controlled.	x		
MA	**Equipment Sanitization**	**L2**	**MA.L2-3.7.3**		**Ensure equipment removed for off-site maintenance is sanitized of any CUI.**			
MA	Equipment Sanitization	L2		MA.L2-3.7.3	equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.	x		
MA	**Media Inspection**	**L2**	**MA.L2-3.7.4**		**Check media containing diagnostic and Test programs for malicious code before the media are used in organizational systems.**			

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
MA	Media Inspection	L2		MA.L2-3.7.4	media containing diagnostic and Test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.	x		
MA	**Nonlocal Maintenance**	**L2**	**MA.L2-3.7.5**		**Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.**			
MA	Nonlocal Maintenance	L2		MA.L2-3.7.5[a]	multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.	x		
MA	Nonlocal Maintenance	L2		MA.L2-3.7.5[b]	nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.	x		
MA	**Maintenance Personnel**	**L2**	**MA.L2-3.7.6**		**Supervise the maintenance activities of personnel without required access authorization.**			
MA	Maintenance Personnel	L2		MA.L2-3.7.6	Determine if maintenance personnel without required access authorization are supervised during maintenance activities.	x		
MP	**Media Protection**	**L2**	**MP.L2-3.8.1**		**Protect [e.g., physically control and securely store] system media containing Federal Contract Information, both paper and digital.**			
MP	Media Protection	L2		MP.L2-3.8.1[a]	paper media containing CUI is physically controlled.	n/a		
MP	Media Protection	L2		MP.L2-3.8.1[b]	digital media containing CUI is physically controlled.	x		
MP	Media Protection	L2		MP.L2-3.8.1[c]	paper media containing CUI is securely stored.	n/a		
MP	Media Protection	L2		MP.L2-3.8.1[d]	digital media containing CUI is securely stored.	x		
MP	**Media Access**	**L2**	**MP.L2-3.8.2**		**Limit access to CUI on system media to authorized users.**			
MP	Media Access	L2		MP.L2-3.8.2	access to CUI on system media is limited to authorized users.	x		
MP	**Media Disposal**	**L1**	**MP.L1-3.8.3**		**Sanitize or destroy information system media containing Federal Contract Information [FCI] before disposal or release for reuse.**			
MP	Media Disposal	L1		MP.L1-3.8.3[a]	system media containing CUI is sanitized or destroyed before disposal.	x		
MP	Media Disposal	L1		MP.L1-3.8.3[b]	system media containing CUI is sanitized before it is released for reuse.	x		
MP	**Media Markings**	**L2**	**MP.L2-3.8.4**		**Mark media with necessary CUI markings and distribution limitations.**			
MP	Media Markings	L2		MP.L2-3.8.4[a]	media containing CUI is marked with applicable CUI markings.	x		
MP	Media Markings	L2		MP.L2-3.8.4[b]	media containing CUI is marked with distribution limitations.	x		
MP	**Media Accountability**	**L2**	**MP.L2-3.8.5**		**Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.**			
MP	Media Accountability	L2		MP.L2-3.8.5[a]	access to media containing CUI is controlled.	x		
MP	Media Accountability	L2		MP.L2-3.8.5[b]	accountability for media containing CUI is maintained during transport outside of controlled areas.	x		
MP	**Portable Storage Encryption**	**L2**	**MP.L2-3.8.6**		**Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.**			
MP	Portable Storage Encryption	L2		MP.L2-3.8.6	the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.	x		
MP	**Removeable Media**	**L2**	**MP.L2-3.8.7**		**Control the use of removable media on system components.**			
MP	Removeable Media	L2		MP.L2-3.8.7	the use of removable media on system components is controlled.	x		
MP	**Shared Media**	**L2**	**MP.L2-3.8.8**		**Prohibit the use of portable storage devices when such devices have no identifiable owner.**			
MP	Shared Media	L2		MP.L2-3.8.8	the use of portable storage devices is prohibited when such devices have no identifiable owner.	x		
MP	**Protect Backups**	**L2**	**MP.L2-3.8.9**		**Protect the confidentiality of backup CUI at storage locations.**			
MP	Protect Backups	L2		MP.L2-3.8.9	the confidentiality of backup CUI is protected at storage locations.	x		
PS	**Screen Individuals**	**L2**	**PS.L2-3.9.1**		**Screen individuals prior to authorizing access to organizational systems containing CUI.**			
PS	Screen Individuals	L2		PS.L2-3.9.1	individuals are screened prior to authorizing access to organizational systems containing CUI.	x	x	OSC CUI users will have to be vetted for MBI
PS	**Personnel Actions**	**L2**	**PS.L2-3.9.2**		**Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.**			ITG will provide related policies, OSC will implement
PS	Personnel Actions	L2		PS.L2-3.9.2[a]	a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.	x	x	
PS	Personnel Actions	L2		PS.L2-3.9.2[b]	system access and credentials are terminated consistent with personnel actions such as termination or transfer.	x	x	
PS	Personnel Actions	L2		PS.L2-3.9.2[c]	the system is protected during and after personnel transfer actions.	x	x	
PE	**Limit Physical Access**	**L1**	**PE.L1-3.10.1**		**Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.**			
PE	Limit Physical Access	L1		PE.L1-3.10.1[a]	authorized individuals allowed physical access are identified.	x		
PE	Limit Physical Access	L1		PE.L1-3.10.1[b]	physical access to organizational systems is limited to authorized individuals.	x		
PE	Limit Physical Access	L1		PE.L1-3.10.1[c]	physical access to equipment is limited to authorized individuals.	x		
PE	Limit Physical Access	L1		PE.L1-3.10.1[d]	physical access to operating environments is limited to authorized individuals.	x		
PE	**Monitor Facility**	**L2**	**PE.L2-3.10.2**		**Protect and monitor the physical facility and support infrastructure for organizational systems.**			
PE	Monitor Facility	L2		PE.L2-3.10.2[a]	the physical facility where organizational systems reside is protected.	x		
PE	Monitor Facility	L2		PE.L2-3.10.2[b]	the support infrastructure for organizational systems is protected.	x		
PE	Monitor Facility	L2		PE.L2-3.10.2[c]	the physical facility where organizational systems reside is monitored.	x		
PE	Monitor Facility	L2		PE.L2-3.10.2[d]	the support infrastructure for organizational systems is monitored.	x		
PE	**Escort Visitors**	**L1**	**PE.L1-3.10.3**		**Escort visitors and monitor visitor activity.**			
PE	Escort Visitors	L1		PE.L1-3.10.3[a]	visitors are escorted.	x		
PE	Escort Visitors	L1		PE.L1-3.10.3[b]	visitor activity is monitored.	x		
PE	**Physical Access Logs**	**L1**	**PE.L1-3.10.4**		**Maintain audit logs of physical access.**			
PE	Physical Access Logs	L1		PE.L1-3.10.4 [a]	audit logs of physical access are maintained.	x		
PE	**Manage Physical Access**	**L1**	**PE.L1-3.10.5**		**Control and manage physical access devices.**			
PE	Manage Physical Access	L1		PE.L1-3.10.5[a]	physical access devices are identified.	x		
PE	Manage Physical Access	L1		PE.L1-3.10.5[b]	physical access devices are controlled.	x		
PE	Manage Physical Access	L1		PE.L1-3.10.5[c]	physical access devices are managed.	x		
PE	**Alternative Work Sites**	**L2**	**PE.L2-3.10.6**		**Enforce safeguarding measures for CUI at alternate work sites.**			
PE	Alternative Work Sites	L2		PE.L2-3.10.6[a]	safeguarding measures for CUI are defined for alternate work sites.	x		
PE	Alternative Work Sites	L2		PE.L2-3.10.6[b]	safeguarding measures for CUI are enforced for alternate work sites.	x		
RA	**Risk Assessments**	**L2**	**RA.L2-3.11.1**		**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.**			
RA	Risk Assessments	L2		RA.L2-3.11.1[a]	the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.	x		
RA	Risk Assessments	L2		RA.L2-3.11.1[b]	risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.	x	x	ITG and OSC will assess risk on a schecheduled freq.
RA	**Vulnerability Scan**	**L2**	**RA.L2-3.11.2**		**Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.**			
RA	Vulnerability Scan	L2		RA.L2-3.11.2[a]	the frequency to scan for vulnerabilities in organizational systems and applications is defined.	x		
RA	Vulnerability Scan	L2		RA.L2-3.11.2[b]	vulnerability scans are performed on organizational systems with the defined frequency.	x		
RA	Vulnerability Scan	L2		RA.L2-3.11.2[c]	vulnerability scans are performed on applications with the defined frequency.	x		

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
RA	Vulnerability Scan	L2		RA.L2-3.11.2[d]	vulnerability scans are performed on organizational systems when new vulnerabilities are identified.	x		
RA	Vulnerability Scan	L2		RA.L2-3.11.2[e]	vulnerability scans are performed on applications when new vulnerabilities are identified.	x		
RA	**Vulnerability Remediation**	**L2**	**RA.L2-3.11.3**		**Remediate vulnerabilities in accordance with risk assessments.**			
RA	Vulnerability Remediation	L2		RA.L2-3.11.3[a]	vulnerabilities are identified.	x		
RA	Vulnerability Remediation	L2		RA.L2-3.11.3[b]	vulnerabilities are remediated in accordance with risk assessments.	x		
CA	**Security Control Assessment**	**L2**	**CA.L2-3.12.1**		**Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.**			
CA	Security Control Assessment	L2		CA.L2-3.12.1[a]	the frequency of security control assessments is defined.	x		
CA	Security Control Assessment	L2		CA.L2-3.12.1[b]	security controls are assessed with the defined frequency to determine if the controls are effective in their application.	x	x	ITG and OCS will conduct assessment
CA	**Plan of Action**	**L2**	**CA.L2-3.12.2**		**Develop and implement plans of action [e.g., POA&M] designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.**			
CA	Plan of Action	L2		CA.L2-3.12.2[a]	deficiencies and vulnerabilities to be addressed by the plan of action are identified.	x		
CA	Plan of Action	L2		CA.L2-3.12.2[b]	a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.	x		
CA	Plan of Action	L2		CA.L2-3.12.2[c]	the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.	x		
CA	**Security Control Monitoring**	**L2**	**CA.L2-3.12.3**		**Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.**			
CA	Security Control Monitoring	L2		CA.L2-3.12.3	Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.	x		
CA	**System Security Plan**	**L2**	**CA.L2-3.12.4**		**Develop, document and periodically update System Security Plans [SSPs] that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.**			
CA	System Security Plan	L2		CA.L2-3.12.4[a]	a system security plan is developed.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[b]	the system boundary is described and documented in the system security plan.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[c]	the system environment of operation is described and documented in the system security plan.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[d]	the security requirements identified and approved by the designated authority as non-applicable are identified.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[e]	the method of security requirement implementation is described and documented in the system security plan.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[f]	the relationship with or connection to other systems is described and documented in the system security plan.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[g]	the frequency to update the system security plan is defined.	x		
CA	System Security Plan	L2		CA.L2-3.12.4[h]	system security plan is updated with the defined frequency.	x		
SC	**Boundary Protection**	**L1**	**SC.L1-3.13.1**		**Monitor, control and protect organizational communications [e.g., information transmitted or received by organizational information systems] at the external boundaries and key internal boundaries of the information systems.**			
SC	Boundary Protection	L1		SC.L1-3.13.1[a]	the external system boundary is defined.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[b]	key internal system boundaries are defined.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[c]	communications are monitored at the external system boundary.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[d]	communications are monitored at key internal boundaries.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[e]	communications are controlled at the external system boundary.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[f]	communications are controlled at key internal boundaries.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[g]	communications are protected at the external system boundary.	x		
SC	Boundary Protection	L1		SC.L1-3.13.1[h]	communications are protected at key internal boundaries.	x		
SC	**Security Engineering**	**L2**	**SC.L2-3.13.2**		**Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.**			
SC	Security Engineering	L2		SC.L2-3.13.2[a]	architectural designs that promote effective information security are identified.	x		
SC	Security Engineering	L2		SC.L2-3.13.2[b]	software development techniques that promote effective information security are identified.	x		
SC	Security Engineering	L2		SC.L2-3.13.2[c]	systems engineering principles that promote effective information security are identified.	x		
SC	Security Engineering	L2		SC.L2-3.13.2[d]	identified architectural designs that promote effective information security are employed.	x		
SC	Security Engineering	L2		SC.L2-3.13.2[e]	identified software development techniques that promote effective information security are employed.	x		
SC	Security Engineering	L2		SC.L2-3.13.2[f]	identified systems engineering principles that promote effective information security are employed.	x		
SC	**Role Separation**	**L2**	**SC.L2-3.13.3**		**Separate user functionality from system management functionality.**			
SC	Role Separation	L2		SC.L2-3.13.3[a]	user functionality is identified.	x		
SC	Role Separation	L2		SC.L2-3.13.3[b]	system management functionality is identified.	x		
SC	Role Separation	L2		SC.L2-3.13.3[c]	user functionality is separated from system management functionality.	x		
SC	**Shared Resource Control**	**L2**	**SC.L2-3.13.4**		**Prevent unauthorized and unintended information transfer via shared system resources.**			
SC	Shared Resource Control	L2		SC.L2-3.13.4	unauthorized and unintended information transfer via shared system resources is prevented.	x	x	ITG will provide training
SC	**Public-Access System Separation**	**L1**	**SC.L1-3.13.5**		**Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.**			
SC	Public-Access System Separation	L1		SC.L1-3.13.5[a]	publicly accessible system components are identified.	x		
SC	Public-Access System Separation	L1		SC.L1-3.13.5[b]	subnetworks for publicly accessible system components are physically or logically separated from internal networks.	x		
SC	**Network Communication by Exception**	**L2**	**SC.L2-3.13.6**		**Deny network communications traffic by default and allow network communications traffic by exception [e.g., deny all, permit by exception].**			
SC	Network Communication by Exception	L2		SC.L2-3.13.6[a]	network communications traffic is denied by default.	x		
SC	Network Communication by Exception	L2		SC.L2-3.13.6[b]	network communications traffic is allowed by exception.	x		
SC	**Split Tunneling**	**L2**	**SC.L2-3.13.7**		**Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks [e.g., split tunneling].**			
SC	Split Tunneling	L2		SC.L2-3.13.7	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).	x		
SC	**Data in Transit**	**L2**	**SC.L2-3.13.8**		**Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.**			
SC	Data in Transit	L2		SC.L2-3.13.8[a]	cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.	x		
SC	Data in Transit	L2		SC.L2-3.13.8[b]	alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.	x		
SC	Data in Transit	L2		SC.L2-3.13.8[c]	either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.	x		

Shared Responsibility Matrix

Domain	Name	Level	Control	Objective	Assessment Objectives	ITG	OSC	Description
SC	**Connections Termination**	**L2**	**SC.L2-3.13.9**		**Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.**			
SC	Connections Termination	L2		SC.L2-3.13.9[a]	a period of inactivity to terminate network connections associated with communications sessions is defined.	x		
SC	Connections Termination	L2		SC.L2-3.13.9[b]	network connections associated with communications sessions are terminated at the end of the sessions.	x		
SC	Connections Termination	L2		SC.L2-3.13.9[c]	network connections associated with communications sessions are terminated after the defined period of inactivity.	x		
SC	**Key Management**	**L2**	**SC.L2-3.13.10**		**Establish and manage cryptographic keys for cryptography employed in organizational systems.**			
SC	Key Management	L2		SC.L2-3.13.10[a]	cryptographic keys are established whenever cryptography is employed.	x		
SC	Key Management	L2		SC.L2-3.13.10[b]	cryptographic keys are managed whenever cryptography is employed.	x		
SC	**CUI Encryption**	**L2**	**SC.L2-3.13.11**		**Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.**			
SC	CUI Encryption	L2		SC.L2-3.13.11	FIPS-validated cryptography is employed to protect the confidentiality of CUI.	x		
SC	**Collaborative Device Control**	**L2**	**SC.L2-3.13.12**		**Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.**			
SC	Collaborative Device Control	L2		SC.L2-3.13.12[a]	collaborative computing devices are identified.	x		
SC	Collaborative Device Control	L2		SC.L2-3.13.12[b]	collaborative computing devices provide indication to users of devices in use.	x		
SC	Collaborative Device Control	L2		SC.L2-3.13.12[c]	remote activation of collaborative computing devices is prohibited.	x		
SC	**Mobile Code**	**L2**	**SC.L2-3.13.13**		**Control and monitor the use of mobile code.**			
SC	Mobile Code	L2		SC.L2-3.13.13[a]	use of mobile code is controlled.	x		
SC	Mobile Code	L2		SC.L2-3.13.13[b]	use of mobile code is monitored.	x		
SC	**Voice over Internet Protocol**	**L2**	**SC.L2-3.13.14**		**Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.**			
SC	Voice over Internet Protocol	L2		SC.L2-3.13.14[a]	use of Voice over Internet Protocol (VoIP) technologies is controlled.	x		
SC	Voice over Internet Protocol	L2		SC.L2-3.13.14[b]	use of Voice over Internet Protocol (VoIP) technologies is monitored.	x		
SC	**Communications Authenticity**	**L2**	**SC.L2-3.13.15**		**Protect the authenticity of communications sessions.**			
SC	Communications Authenticity	L2		SC.L2-3.13.15	the authenticity of communications sessions is protected.	x		
SC	**Data at Rest**	**L2**	**SC.L2-3.13.16**		**Protect the confidentiality of CUI at rest.**			
SC	Data at Rest	L2		SC.L2-3.13.16	the confidentiality of CUI at rest is protected.	x		
SI	**Flaw Remediation**	**L1**	**SI.L1-3.14.1**		**Identify, report and correct information and information system flaws in a timely manner.**			
SI	Flaw Remediation	L1		SI.L1-3.14.1[a]	the time within which to identify system flaws is specified.	x		
SI	Flaw Remediation	L1		SI.L1-3.14.1[b]	system flaws are identified within the specified time frame.	x		
SI	Flaw Remediation	L1		SI.L1-3.14.1[c]	the time within which to report system flaws is specified.	x		
SI	Flaw Remediation	L1		SI.L1-3.14.1[d]	system flaws are reported within the specified time frame.	x		
SI	Flaw Remediation	L1		SI.L1-3.14.1[e]	the time within which to correct system flaws is specified.	x		
SI	Flaw Remediation	L1		SI.L1-3.14.1[f]	system flaws are corrected within the specified time frame.	x		
SI	**Malicious Code Protection**	**L1**	**SI.L1-3.14.2**		**Provide protection from malicious code at appropriate locations within organizational information systems.**			
SI	Malicious Code Protection	L1		SI.L1-3.14.2[a]	designated locations for malicious code protection are identified.	x		
SI	Malicious Code Protection	L1		SI.L1-3.14.2[b]	protection from malicious code at designated locations is provided.	x		
SI	**Security Alerts & Advisories**	**L2**	**SI.L2-3.14.3**		**Monitor system security alerts and advisories and take action in response.**			
SI	Security Alerts & Advisories	L2		SI.L2-3.14.3[a]	response actions to system security alerts and advisories are identified.	x		
SI	Security Alerts & Advisories	L2		SI.L2-3.14.3[b]	system security alerts and advisories are monitored.	x		
SI	Security Alerts & Advisories	L2		SI.L2-3.14.3[c]	actions in response to system security alerts and advisories are taken.	x		
SI	**Update Malicious Code Protection**	**L1**	**SI.L1-3.14.4**		**Update malicious code protection mechanisms when new releases are available.**			
SI	Update Malicious Code Protection	L1		SI.L1-3.14.4	Determine if malicious code protection mechanisms are updated when new releases are available.	x		
SI	**System & File Scanning**	**L1**	**SI.L1-3.14.5**		**Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.**			
SI	System & File Scanning	L1		SI.L1-3.14.5[a]	the frequency for malicious code scans is defined.	x		
SI	System & File Scanning	L1		SI.L1-3.14.5[b]	malicious code scans are performed with the defined frequency.	x		
SI	System & File Scanning	L1		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.	x		
SI	**Monitor Communications for Attacks**	**L2**	**SI.L2-3.14.6**		**Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.**			
SI	Monitor Communications for Attacks	L2		SI.L2-3.14.6[a]	the system is monitored to detect attacks and indicators of potential attacks.	x		
SI	Monitor Communications for Attacks	L2		SI.L2-3.14.6[b]	inbound communications traffic is monitored to detect attacks and indicators of potential attacks.	x		
SI	Monitor Communications for Attacks	L2		SI.L2-3.14.6[c]	outbound communications traffic is monitored to detect attacks and indicators of potential attacks.	x		
SI	**Identify Unauthorized Use**	**L2**	**SI.L2-3.14.7**		**Identify unauthorized use of organizational systems.**			
SI	Identify Unauthorized Use	L2		SI.L2-3.14.7[a]	authorized use of the system is defined.	x		
SI	Identify Unauthorized Use	L2		SI.L2-3.14.7[b]	unauthorized use of the system is identified.	x		