#	CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Relationship	NIST SP 800-53r5 Control Identifier	Control (and Control Enhancement) Name	Control Statement	Privacy Baseline	Low Baseline	Moderate Baseline	High Baseline	No Baseline	New	Corrected
1	**1**				**Inventory and Control of Hardware Assets**	**Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.**													
2	1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x	Subset	CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system 2. Includes all components within the system		x	x	x			
3	1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x	Superset	CM-8(1)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.			x	x			
4	1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x	Subset	PM-5	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.			N/A - Deployed organization-wide		x		
5	1	1.2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x	Subset	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].			x	x			
6	1	1.3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		x	x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];		x	x	x			
7	1	1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		x	x	Subset	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].			x	x			
8	1	1.5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x	Subset	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].			x	x			
9	1	1.5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];		x	x	x			
10	**2**				**Inventory and Control of Software Assets**	**Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**													
11	2	2.1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	x	x	x	Subset	CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system;		x	x	x			
12	2	2.1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	x	x	x	Subset	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].			x	x			
13	2	2.1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	x	x	x	Superset	MA-3	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].			x	x			
14	2	2.2	Applications	Identify	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	x	x	x	Equivalent	SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].		x	x	x			
15	2	2.3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x	Subset	CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].			x	x			
16	2	2.3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x	Subset	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].			x	x			

17	2	2.3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x	Subset	CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		x	x	x			x
18	2	2.3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x	Subset	CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].		x	x	x			
19	2	2.4	Applications	Detect	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		x	x	Subset	CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].			x	x			
20	2	2.5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		x	x	Equivalent	CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].		x	x	x			x
21	2	2.5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		x	x	Superset	CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		x	x	x			
22	2	2.6	Applications	Protect	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			
23	2	2.6	Applications	Protect	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		x	x	Superset	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].			x	x			
24	2	2.7	Applications	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			
25	2	2.7	Applications	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x	Superset	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].			x	x			
26	2	2.7	Applications	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x	Superset	SI-7	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].			x	x			
27	2	2.7	Applications	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x	Superset	SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].			x	x			
28	**3**				**Data Protection**	**Operate processes and tooling to control, handle, retain, and dispose the enterprise's data.**														
29	3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	x	x	x	x			x
30	3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.			x				
31	3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Equivalent	SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	x	x	x	x			x
32	3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	Superset	CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.			x				
33	3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	Superset	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	x		N/A - Deployed organization-wide		x		
34	3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	Superset	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	x		N/A - Deployed organization-wide				
35	3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	Superset	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	x		N/A - Deployed organization-wide				

36	3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x	Subset	RA-2	Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.		x	x	x			x
37	3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x	Subset	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.		x	x	x			
38	3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x	Subset	AC-5	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.			x	x			
39	3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x	Subset	AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.			x	x			
40	3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x	Superset	MP-2	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].		x	x	x			
41	3	3.4	Data	Protect	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	x	x	x	Subset	AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	x	x	x	x			
42	3	3.4	Data	Protect	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	x	x	x	Subset	SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	x	x	x	x			
43	3	3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	x	x	x	Subset	MP-6	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	x	x	x	x			
44	3	3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	x	x	x	Subset	SR-12	Component Disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].		x	x	x			
45	3	3.6	Devices	Protect	Encrypt Data on End-User Devices	Encrypt data on end user devices, including workstations, laptops, tablets, and smartphones containing sensitive data. Example implementations include, but are not limited to, Windows BitLocker, Apple FileVault, Linux dm-crypt.	x	x	x	Subset	SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].			x	x			
46	3	3.7	Devices	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	RA-2	Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.		x	x	x			
47	3	3.8	Data	Identify	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].			x				
48	3	3.8	Data	Identify	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.			x				
49	3	3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		x	x	Subset	MP-5	Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.			x	x			
50	3	3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		x	x	Subset	MP-7	Media Use	a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls];		x	x	x			
51	3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	Subset	AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.			x	x			
52	3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	Subset	IA-5	Authenticator Management	g. Protecting authenticator content from unauthorized disclosure and modification;		x	x	x			
53	3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	Subset	IA-5(1)	Authenticator Management | Password-based Authentication	(c) Transmit passwords only over cryptographically-protected channels;		x	x	x			
54	3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	Subset	SC-8	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.			x	x			
55	3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x	Subset	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.			x	x			
56	3	3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		x	x	Superset	IA-5(1)	Authenticator Management | Password-based Authentication	(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;		x	x	x			
57	3	3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		x	x	Equivalent	SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].			x	x			
58	3	3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		x	x	Superset	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].			x	x			
59	3	3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		x	x	Superset	AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.					x	x	
60	3	3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		x	x	Superset	CP-9(3)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.				x		x	
61	3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			x	Subset	CA-7	Continuous Monitoring	d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;	x	x	x	x			

62	3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			x	Subset	CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.			x	x			
63	3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			x	Subset	CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.			x	x			
64	3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			x	Subset	SC-4	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.			x	x			
65	3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x	Subset	AC-6(9)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.			x	x			
66	3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x	Subset	AU-2	Event Logging	c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];	x	x	x	x			
67	3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x	Subset	AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.		x	x	x			
68	**4**				**Secure Configuration of Enterprise Assets and Software**	**Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).**															
69	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Equivalent	CM-1	Policy and Procedures	2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;	x	x	x	x			
70	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;		x	x	x			
71	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings;		x	x	x			
72	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities];		x	x	x			
73	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].			x	x			
74	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Equivalent	CM-9	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and e. Protects the configuration management plan from unauthorized disclosure and modification.			x	x			
75	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	x	x	x	x			
76	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].		x	x	x			
77	4	4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].			x	x			
78	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.		x	x	x			
79	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	AC-18(1)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.			x	x			
80	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	AC-18(3)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.			x	x			
81	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;		x	x	x			x

82	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x			x
83	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			x
84	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CM-7(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].			x	x			
85	4	4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Equivalent	CM-9	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and e. Protects the configuration management plan from unauthorized disclosure and modification.			x	x			
86	4	4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x	Subset	AC-2(5)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].			x	x			
87	4	4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x	Equivalent	AC-11	Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.			x	x			
88	4	4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x	Superset	AC-11(1)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.			x	x			
89	4	4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x	Superset	AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].			x	x			
90	4	4.4	Devices	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	x	x	x	Subset	CA-9	Internal System Connections	b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;		x	x	x			
91	4	4.4	Devices	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	x	x	x	Subset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		x	x	x			
92	4	4.4	Devices	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	x	x	x	Subset	SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].			x	x			
93	4	4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	x	x	x	Subset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		x	x	x			
94	4	4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	x	x	x	Subset	SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].			x	x			
95	4	4.6	Network	Protect	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	x	x	x	Superset	MA-4	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintain records for nonlocal maintenance and diagnostic activities; and e. Terminate session and network connections when nonlocal maintenance is completed.		x	x	x			
96	4	4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	x	x	x	Subset	IA-5	Authenticator Management	e. Changing default authenticators prior to first use;		x	x	x			
97	4	4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		x	x	Subset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x			
98	4	4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			

99	4	4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		x	x	Subset	SC-20	Secure Name/address Resolution Service (authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.		x	x	x			
100	4	4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		x	x	Subset	SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.		x	x	x			
101	4	4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		x	x	Subset	SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.		x	x	x			
102	4	4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		x	x	Subset	AC-7	Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]		x	x	x			
103	4	4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		x	x	Subset	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.		x	x	x			
104	4	4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		x	x	Subset	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.		x	x	x			
105	4	4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		x	x	Subset	AC-20	Use of External Systems	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organizationally-defined types of external systems].		x	x	x			
106	4	4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			x	Equivalent	AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].			x	x			
106.1	4	4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			x	Subset	MP-4	Media Storage	a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.			x	x		x	
107	4	4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			x	Subset	SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.		x	x	x			x
108	**5**				**Account Management**	**Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.**															
109	5	5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	x	x	x	Subset	AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management		x	x	x			
110	5	5.2	Users	Protect	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	x	x	x	Subset	IA-5(1)	Authenticator Management | Password-based Authentication	(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators; and (h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].		x	x	x			
111	5	5.3	Users	Respond	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	x	x	x	Subset	AC-2(3)	Account Management | Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].			x	x			
112	5	5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	x	x	x	Superset	AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.			x	x			
113	5	5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	x	x	x	Superset	AC-6(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].			x	x			

114	5	5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		x	x	Subset	AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management		x	x	x			
115	5	5.6	Users	Protect	Centralize Account Management	Centralize account management through a directory or identity service.		x	x	Subset	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].			x	x			
116	**6**				**Access Control Management**	**Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.**															
117	6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Subset	IA-4	Identifier Management	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device;		x	x	x			
118	6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Subset	IA-5	Authenticator Management	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;		x	x	x			
119	6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Subset	AC-1	Policy and Procedures	3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];	x	x	x	x			
120	6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Subset	AC-2	Account Management	f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];		x	x	x			
121	6	6.1	Users	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	x	x	Subset	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].			x	x			
122	6	6.2	Users	Protect	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	x	x	Subset	AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	x	x	x	x			
123	6	6.2	Users	Protect	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	x	x	Subset	AC-2	Account Management	k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.		x	x	x			
124	6	6.2	Users	Protect	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	x	x	Subset	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].			x	x			
125	6	6.3	Users	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	x	x	x	Subset	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.		x	x	x			
126	6	6.3	Users	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	x	x	x	Subset	IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.		x	x	x			
127	6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x	Subset	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.		x	x	x			
128	6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x	Subset	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.		x	x	x			
129	6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x	Subset	IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.		x	x	x			
130	6	6.5	Users	Protect	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	x	x	x	Equivalent	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.		x	x	x			

131	6	6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		x	x	Subset	CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b. Review and update the system component inventory [Assignment: organization-defined frequency].		x	x	x			
132	6	6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		x	x	Subset	IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.		x	x	x			
133	6	6.7	Users	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		x	x	Subset	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].			x	x			
134	6	6.7	Users	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		x	x	Subset	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.		x	x	x			
135	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Subset	AC-2	Account Management	2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];		x	x	x			
136	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Subset	AC-5	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.			x	x			
137	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Subset	AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.			x	x			
138	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Superset	AC-6(1)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information].			x	x			
139	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Subset	AC-6(7)	Least Privilege | Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.			x	x			
140	6	6.8	Data	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x	Superset	AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].			x	x			
141	**7**				**Continuous Vulnerability Management**	**Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.**															
142	7	7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact;		x	x	x			
143	7	7.2	Applications	Respond	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	x	x	x	Superset	RA-5	Vulnerability Monitoring and Scanning	c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x			
144	7	7.3	Applications	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x			
145	7	7.3	Applications	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	x	x	x	x			
146	7	7.3	Applications	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	SI-2	Flaw Remediation	c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and		x	x	x			
147	7	7.3	Applications	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].			x	x			

148	7	7.4	Applications	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x			
149	7	7.4	Applications	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	x	x	x	x			
150	7	7.4	Applications	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	SI-2	Flaw Remediation	c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and		x	x	x			
151	7	7.4	Applications	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x	Subset	SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].			x	x			
152	7	7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact;		x	x	x			
153	7	7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact;		x	x	x			
154	7	7.7	Applications	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact;		x	x	x			
155	7	7.7	Applications	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		x	x	Superset	RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].		x	x	x			
156	7	7.7	Applications	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		x	x	Subset	RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	x	x	x	x			
157	7	7.7	Applications	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		x	x	Subset	SI-2	Flaw Remediation	a. Identify, report, and correct system flaws;		x	x	x			
158	**8**				**Audit Log Management**	**Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.**															
159	8	8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Equivalent	AU-1	Policy and Procedures	2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;	x	x	x	x			
160	8	8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	AU-2	Event Logging	c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];	x	x	x	x			
161	8	8.2	Network	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	x	x	x	Equivalent	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;	x	x	x	x			
162	8	8.2	Network	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging has been enabled across end-user devices, applications, and network infrastructure.	x	x	x	Subset	AU-7	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.			x	x			
163	8	8.2	Network	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging has been enabled across end-user devices, applications, and network infrastructure.	x	x	x	Equivalent	AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];		x	x	x			
164	8	8.3	Network	Protect	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	x	x	x	Equivalent	AU-4	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].		x	x	x			

165	8	8.4	Network	Protect	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		x	x	Subset	AU-8	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.		x	x	x			
166	8	8.5	Network	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x	Equivalent	AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.		x	x	x			
167	8	8.5	Network	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x	Subset	AU-3(1)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].			x	x			
168	8	8.5	Network	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x	Subset	AU-7	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.			x	x			
169	8	8.5	Network	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x	Subset	AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];		x	x	x			
170	8	8.6	Network	Detect	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.		x	x	Subset	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	x	x	x	x			
171	8	8.7	Network	Detect	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.		x	x	Subset	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	x	x	x	x			
172	8	8.8	Network	Detect	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		x	x	Subset	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	x	x	x	x			
173	8	8.9	Devices	Detect	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.		x	x	Subset	AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.			x	x			
174	8	8.10	Network	Protect	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.		x	x	Equivalent	AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	x	x	x	x			
175	8	8.11	Network	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		x	x	Equivalent	AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;		x	x	x			
176	8	8.11	Network	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		x	x	Subset	AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].			x	x			
177	8	8.11	Network	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		x	x		AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].			x	x			
178	8	8.12	Data	Detect	Collect Service Provider Logs	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.			x	Subset	AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	x	x	x	x			
179	**9**				**Email and Web Browser Protections**	**Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.**															

180	9	9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	x	x	x	Subset	CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		x	x	x			
181	9	9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	x	x	x	Subset	SC-18	Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.			x	x			x
182	9	9.2	Network	Protect	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	x	x	x	Superset	SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.			x	x			
183	9	9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		x	x	Subset	SC-7(3)	Boundary Protection | Access Points	Limit the number of external network connections to the system.			x	x			x
184	9	9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		x	x	Subset	SC-7(4)	Boundary Protection | External Telecommunications Services	(h) Filter unauthorized control plane traffic from external networks.			x	x			x
185	9	9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		x	x	Subset	CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		x	x	x			x
186	9	9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		x	x	Subset	CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].		x	x	x			x
187	9	9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		x	x	Subset	SC-18	Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.			x	x			
188	9	9.5	Network	Protect	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		x	x	Subset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		x	x	x			
189	9	9.6	Network	Protect	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		x	x	Subset	SI-3	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.		x	x	x			
190	9	9.6	Network	Protect	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		x	x	Subset	SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.			x	x			
191	9	9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			x	Subset	SI-3	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.		x	x	x			
192	9	9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			x	Subset	SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.			x	x			
193	**10**				**Malware Defenses**	**Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.**															
194	10	10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	x	x	x	Subset	SI-3	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;		x	x	x			
195	10	10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	x	x	x	Subset	SI-3	Malicious Code Protection	b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;		x	x	x			

196	10	10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	x	x	x	Subset	MP-7	Media Use	a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.		x	x	x			
197	10	10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.		x	x	Subset	MP-7	Media Use	a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.		x	x	x			
198	10	10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.		x	x	Subset	SI-3	Malicious Code Protection	1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and		x	x	x			
199	10	10.5	Devices	Protect	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		x	x	Superset	SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].			x	x			
200	10	10.6	Devices	Protect	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.		x	x	Subset	SI-3	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.		x	x	x			
201	10	10.7	Devices	Detect	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.		x	x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		x	x	x			
202	**11**				**Data Recovery**	**Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.**															
203	11	11.1	Data	Recover	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CP-2	Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [Assignment: organization-defined frequency]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; g. Incorporate lessons learned from contingency plan testing,		x	x	x			
204	11	11.1	Data	Recover	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.		x	x	x			
205	11	11.2	Data	Recover	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	x	x	x	Subset	CP-9	System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];		x	x	x			
206	11	11.2	Data	Recover	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	x	x	x	Subset	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.		x	x	x			
207	11	11.3	Data	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	x	x	x	Subset	CP-9	System Backup	d. Protect the confidentiality, integrity, and availability of backup information.		x	x	x			
208	11	11.3	Data	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	x	x	x	Subset	CP-9(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].			x	x			
209	11	11.3	Data	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	x	x	x	Subset	SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].			x	x			

210	11	11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	x	x	x	Superset	CP-6	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.			x	x			
211	11	11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	x	x	x	Superset	CP-6(1)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.			x	x			
212	11	11.5	Data	Recover	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		x	x	Subset	CP-4	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan:		x	x	x			
213	11	11.5	Data	Recover	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		x	x	Subset	CP-9(1)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.			x	x			
214	**12**				**Network Infrastructure Management**	**Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.**															
215	12	12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	x	x	x	Subset	CM-8(1)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.			x	x			
216	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Subset	PL-8	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	x		x	x			
217	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Subset	PM-7	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	x		N/A - Deployed organization-wide		x		
218	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Subset	SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].		x	x	x			
219	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Superset	CM-7	Least Functionality	b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			
220	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Superset	CP-6	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.			x	x			
221	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Superset	CP-7	Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.			x	x			
222	12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		x	x	Superset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		x	x	x			
223	12	12.3	Network	Protect	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		x	x	Subset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x			x
224	12	12.3	Network	Protect	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			x
225	12	12.3	Network	Protect	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		x	x	Subset	SC-23	Session Authenticity	Protect the authenticity of communications sessions.			x	x			
226	12	12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	PL-8	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	x		x	x			

227	12	12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	PM-5	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.			N/A - Deployed organization-wide		x		
228	12	12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.		x	x	Subset	AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].			x	x			
229	12	12.6	Network	Protect	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		x	x	Subset	AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.		x	x	x			
230	12	12.6	Network	Protect	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		x	x	Subset	SC-23	Session Authenticity	Protect the authenticity of communications sessions.			x	x			
231	12	12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		x	x	Subset	AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.		x	x	x			
232	12	12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		x	x	Subset	AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.			x	x			
233	12	12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		x	x	Subset	AC-17(3)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.			x	x			
234	12	12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			x	Superset	SC-7(15)	Boundary Protection | Network Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.					x	x	
235	**13**				**Network Monitoring and Defense**	**Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.**															
236	13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x	Subset	AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].			x	x			
237	13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x	Subset	AU-7	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.			x	x			
238	13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x	Superset	IR-4(1)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [Assignment: organization-defined automated mechanisms].			x	x			
239	13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x	Superset	SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.			x	x			
240	13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x	Subset	SI-4(5)	System Monitoring | System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].			x	x			
241	13	13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		x	x	Subset	SC-7(12)	Boundary Protection | Host-Based Protection	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].					x	x	
242	13	13.3	Network	Detect	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		x	x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;		x	x	x			
243	13	13.3	Network	Detect	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		x	x	Subset	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].			x	x			
244	13	13.4	Network	Protect	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.		x	x	Subset	CA-9	Internal System Connections	b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;		x	x	x			
245	13	13.4	Network	Protect	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.		x	x	Subset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;		x	x	x			
246	13	13.5	Devices	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		x	x	Subset	AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.		x	x	x			
247	13	13.5	Devices	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		x	x	Subset	AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.			x	x			
248	13	13.5	Devices	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		x	x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;		x	x	x			
249	13	13.5	Devices	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		x	x	Subset	SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		x	x	x			
250	13	13.6	Network	Detect	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		x	x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;		x	x	x			
251	13	13.6	Network	Detect	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		x	x	Superset	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].			x	x			
252	13	13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.			x	Subset	SC-7(12)	Boundary Protection | Host-Based Protection	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].					x	x	
253	13	13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;		x	x	x			

254	13	13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			x	Subset	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].			x	x			
255	13	13.9	Devices	Protect	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			x	Subset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x			
256	13	13.9	Devices	Protect	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			
257	13	13.10	Network	Protect	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			x	Superset	SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.			x	x			
258	13	13.11	Network	Detect	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.			x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;		x	x	x			
259	**14**				**Security Awareness and Skills Training**	**Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.**															
260	14	14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	AT-1	Policy and Procedures	1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: c. Review and update the current awareness and training:	x	x	x	x			
261	14	14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
262	14	14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	x		N/A - Deployed organization-wide		x		
263	14	14.2	N/A	Protect	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	x	x	x	Equivalent	AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.			x	x			
264	14	14.3	N/A	Protect	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
265	14	14.4	N/A	Protect	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
266	14	14.5	N/A	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	x	x	x	Subset	AC-22	Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;		x	x	x			
267	14	14.6	N/A	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
268	14	14.7	N/A	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
269	14	14.8	N/A	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	x	x	x	Subset	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors	x	x	x	x			
270	14	14.9	N/A	Protect	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.		x	x	Equivalent	AT-3	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:	x	x	x	x			
271	**15**				**Service Provider Management**	**Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.**															
272	15	15.1	N/A	Identify	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	PM-30(1)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.			N/A - Deployed organization-wide		x		
273	15	15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.			x	x			
274	15	15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	SA-9	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]	x	x	x	x			
275	15	15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].			x	x			
276	15	15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	PM-30	Supply Chain Risk Management Strategy	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; 1. Implement the supply chain risk management strategy consistently across the organization; and (a) Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.			N/A - Deployed organization-wide		x		

277	15	15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	SR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].		x	x	x			
278	15	15.2	N/A	Identify	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	AC-20	Use of External Systems	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organizationally-defined types of external systems].		x	x	x			
279	15	15.2	N/A	Identify	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].			x	x			
280	15	15.3	N/A	Identify	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		x	x	Subset	AC-20(1)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or (b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.			x	x			
281	15	15.3	N/A	Identify	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		x	x	Subset	AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].			x	x			
282	15	15.3	N/A	Identify	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		x	x	Subset	PM-17	Protecting Controlled Unclassified Information on External Systems	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and b. Review and update the policy and procedures [Assignment: organization-defined frequency].	x		N/A - Deployed organization-wide		x		
283	15	15.3	N/A	Identify	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		x	x	Subset	SR-5	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].		x	x	x			
284	15	15.4	N/A	Protect	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.		x	x	Subset	SA-4	Acquisition Process	a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management;	x	x	x	x			
285	15	15.4	N/A	Protect	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.		x	x	Subset	SR-5	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].		x	x	x			
286	15	15.4	N/A	Protect	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.		x	x	Subset	SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].			x	x			
287	15	15.5	N/A	Identify	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.			x	Subset	AC-20(1)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or (b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.			x	x			

288	15	15.5	N/A	Identify	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.			x	Subset	SI-4	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		x	x	x			x
289	15	15.6	N/A	Identify	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.			x	Subset	SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].			x	x			
290	15	15.7	Data	Protect	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation; termination of data flows; and secure disposal of enterprise data within service provider systems.			x	Subset	SA-9	External Systems Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	x	x	x	x		x	
291	**16**				**Application Software Security**	**Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.**															
292	16	16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	x	x	x	x			
293	16	16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].			x	x			
294	16	16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		x	x	Superset	CA-5	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	x	x	x	x			
295	16	16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		x	x	Subset	RA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	x	x	x	x			

296	16	16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x			
297	16	16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		x	x	Subset	RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	x	x	x	x			
298	16	16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.		x	x	Subset	SI-2	Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.		x	x	x			
299	16	16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.		x	x	Subset	CM-8	System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b. Review and update the system component inventory [Assignment: organization-defined frequency].		x	x	x			x
300	16	16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		x	x	Subset	SR-11	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].		x	x	x			
301	16	16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.		x	x	Subset	RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		x	x	x			
302	16	16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.		x	x	Subset	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		x	x	x			
303	16	16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.		x	x	Subset	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].		x	x	x			
304	16	16.8	Applications	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.		x	x	Superset	CM-4(1)	Impact Analyses | Separate Test Environments	nalyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.				x		x	
305	16	16.8	Applications	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.		x	x	Superset	SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.					x	x	

306	16	16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.		x	x	Subset	SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].		x	x	x			
307	16	16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.		x	x	Subset	PL-8	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	x	x	x	x			
308	16	16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.		x	x	Subset	SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].		x	x	x			
309	16	16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		x	x	Subset	SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].			x	x			
310	16	16.12	Applications	Protect	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.			x	Subset	SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.	x		x	x			
311	16	16.12	Applications	Protect	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.			x	Subset	SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].			x	x			
312	16	16.13	Applications	Protect	Conduct Application Penetration Testing	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.			x	Subset	CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].				x		x	
313	16	16.14	Applications	Protect	Conduct Threat Modeling	Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.			x	Subset	SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analysis	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; b. Employs the following tools and methods: [Assignment: organization-defined tools and methods]; c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and d. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].					x	x	
314	**17**				**Incident Response Management**	**Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.**															
315	17	17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	IR-1	Policy and Procedures	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and	x	x	x	x			
316	17	17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Superset	IR-7	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	x	x	x	x			
317	17	17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	IR-8	Incident Response Plan	10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];	x	x	x	x			

318	17	17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	x	x	x	Subset	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	x	x	x	x			
319	17	17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	x	x	x	Subset	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	x	x	x	x			
320	17	17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	x	x	x	Superset	IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.			x	x			
321	17	17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x	Subset	IR-5	Incident Monitoring	Track and document incidents.	x	x	x	x			
322	17	17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	x	x	x	x			
323	17	17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	IR-6(1)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].			x	x			
324	17	17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-8	Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and	x	x	x	x			
325	17	17.4	N/A	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-1	Policy and Procedures	c. Review and update the current incident response:	x	x	x	x			
326	17	17.4	N/A	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	IR-6(1)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].			x	x			
327	17	17.4	N/A	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	x	x	x	x			x
328	17	17.4	N/A	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	IR-6(1)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].			x	x			
329	17	17.4	N/A	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-8	Incident Response Plan	2. Describes the structure and organization of the incident response capability; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;	x	x	x	x			
330	17	17.5	N/A	Respond	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-1	Policy and Procedures	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and	x	x	x	x			
331	17	17.5	N/A	Respond	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-8	Incident Response Plan	10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];	x	x	x	x			
332	17	17.6	N/A	Respond	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Superset	CP-8	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.			x	x			
333	17	17.6	N/A	Respond	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x	Subset	IR-8	Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and	x	x	x	x			x

334	17	17.7	N/A	Recover	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.		x	x	Equivalent	IR-3	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	x		x	x			
335	17	17.8	N/A	Recover	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.		x	x	Subset	IR-4	Incident Handling	c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and	x	x	x	x			
336	17	17.9	N/A	Recover	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			x	Subset	IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].	x	x	x	x			
337	17	17.9	N/A	Recover	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			x	Subset	IR-8	Incident Response Plan	5. Defines reportable incidents;	x	x	x	x			
338	18				**Penetration Testing**	**Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.**															
339	18	18.1	N/A	Identify	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics should include scope, such as network, web application, API, hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and, retrospective requirements.		x	x	Equivalent	CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].				x		x	
340	18	18.2	Network	Identify	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, but no less than annually. External penetration testing should include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted by a qualified party. The testing may be clear box or opaque box. See the Cloud Companion Guide for cloud-specific guidance.		x	x	Superset	CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.				x		x	
341	18	18.3	Network	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.		x	x	Subset	SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.					x	x	
342	18	18.3	Network	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.		x	x	Subset	PM-4	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	x				x	x	
343	18	18.4	Network	Protect	Validate Security Measures	Validate security measures after each penetration test. Enterprises should modify rulesets and capabilities to detect the techniques used by testers.			x	Subset	PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	x				x	x	
344	18	18.4	Network	Protect	Validate Security Measures	Validate security measures after each penetration test. Enterprises should modify rulesets and capabilities to detect the techniques used by testers.			x	Subset	SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.					x	x	
345	18	18.5	N/A	Identify	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, but no less than annually. The testing may be clear box or opaque box. See the Cloud Companion Guide for cloud-specific guidance.			x	Subset	CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].				x		x	