Policy to CIS Critical Security Controls Mapping						CJIS	PCI v4.0	NIST 800-53 Moderate
1	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	1	Asset Management Policy	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.	5.4, 5.13.1.1, 5.13.1.2, 5.13.1.3	9.5.1, 9.5.1.1, 11.2, 11.2.1, 11.2.2, 12.5, 12.5.1	CM-8(1)
1	1.2	Address Unauthorized Assets	1	Asset Management Policy	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.	5.4.1.1.1, 5.4.3, 5.5.6	11.2.1	CM-8(3)
1	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	2	Asset Management Policy	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.	5.4		CM-8(3)
1	1.5	Use a Passive Asset Discovery Tool	3	Asset Management Policy	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.			CM-8(3)
2	2.1	Establish and Maintain a Software Inventory	1	Asset Management Policy	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, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.	5.4	1.2.5, 6.3.2	CM-7(1), MA-3
2	2.2	Ensure Authorized Software is Currently Supported	1		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.	5.4	2.2.5, 12.3.4	
2	2.3	Address Unauthorized Software	1		Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	5.4.1, 5.4.1.1.1	12.3.4	CM-10, CM-7(2), CM-8(3)
2	2.4	Utilize Automated Software Inventory Tools	2		Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.			CM-8(3)
2	2.5	Allowlist Authorized Software	2		Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	5.7.1.1	1.2.5, 2.2.4	CM-7(5)
2	2.6	Allowlist Authorized Libraries	2		Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		1.2.5, 2.2.4	CM-7(1)
2	2.7	Allowlist Authorized Scripts	3		Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.		1.2.5, 2.2.4, 6.4.3	CM-7(1), SI-7, SI-7(1)
3	3.1	Establish and Maintain a Data Management Process	1	Data Management Policy	Establish and maintain a documented 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	5.1.1.1	9.4, 9.4.2	AU-11, CM-12, SI-12
3	3.2	Establish and Maintain a Data Inventory	1	Data Management Policy	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.		3.2.1, 9.4.2, 9.4.5.1, 12.5.2	CM-12
3	3.3	Configure Data Access Control Lists	1	Data Management Policy	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.	5.5.2.1, 5.5.2.3, 5.	1.3.1, 7.1	AC-5, AC-6
3	3.4	Enforce Data Retention	1	Data Management Policy	Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.	5.3.4, 5.4.6	3.2.1	

3	3.5	Securely Dispose of Data	1	Data Management Policy	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	5.8.3	3.2.1, 9.4.6, 9.4.7	
3	3.6	Encrypt Data on End-User Devices	1	Data Management Policy	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	5.13.2, 5.13.3		SC-28
3	3.7	Establish and Maintain a Data Classification Scheme	2	Data Management Policy	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.		9.4.2	
3	3.8	Document Data Flows	2	Data Management Policy	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.	5.10.1	1.2.4, 1.3.1, 1.3.2, 12.5.2	AC-4, CM-12
3	3.9	Encrypt Data on Removable Media	2	Data Management Policy	Encrypt data on removable media.	5.8.1, 5.8.2, 5.8.2.1	3.5.1.2	MP-5
3	3.10	Encrypt Sensitive Data in Transit	2	Data Management Policy	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	5.10.1, 5.10.1.2.1, 5.13.1.1, 5.13.1.4	2.2.7, 4.1.1, 4.2.1, 4.2.1.2, 4.2.2, 8.3.2	AC-17(2), SC-8, SC-8(1)
3	3.11	Encrypt Sensitive Data at Rest	2	Data Management Policy	Encrypt sensitive data at rest on servers, applications, and databases. 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.	5.10.1.2.2	3.1.1, 3.3.2, 3.3.3, 3.5.1, 3.5.1.2, 3.5.1.3, 8.3.2	SC-28, SC-28(1)
3	3.12	Segment Data Processing and Storage Based on Sensitivity	2	Data Management Policy	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.	5.10.3.1, 5.5.6.1, 5.5.6.2	1.4.1, 1.4.4	
3	3.13	Deploy a Data Loss Prevention Solution	3	Data Management Policy	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 data inventory.	5.1.1.1, 5.4.3	10.2.1, 10.2.1.1	CM-12, CM-12(1), SC-4
3	3.14	Log Sensitive Data Access	3	Data Management Policy	Log sensitive data access, including modification and disposal.	5.4.1.1	1.4.1, 1.4.4	AC-6(9)
4	4.1	Establish and Maintain a Secure Configuration Process	1	Secure Configuration Management Policy	Establish and maintain a documented 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.	5.10.1, 5.13.1.1, 5.13.1.2, 5.13.1.2.1, 5.13.1.3, 5.13.2, 5.13.4, 5.13.7.3, 5.7.1, 5.7.2	1.1.1, 1.2.1, 1.2.6, 1.2.7, 1.5.1, 2.1.1, 2.2.1	CM-7(1), CM-9, SA-10
4	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	1	Secure Configuration Management Policy	Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	5.13.1.4	1.1.1, 1.2.1, 1.2.6, 1.2.7, 1.4.2, 1.5.1, 2.1.1, 2.2.1	AC-18(1), AC-18(3), CM-2, CM-6, CM-7, CM-7(1), CM-9
4	4.3	Configure Automatic Session Locking on Enterprise Assets	1	Secure Configuration Management Policy	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.	5.5.5	8.2.8	AC-11, AC-11(1), AC-12, AC-2(5)
4	4.4	Implement and Manage a Firewall on Servers	1	Secure Configuration Management Policy	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	5.10.1, 5.10.4.3, 5.7.1.1	1.2.1, 1.4.1	SC-7(5)
4	4.5	Implement and Manage a Firewall on End-User Devices	1	Secure Configuration Management Policy	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.	5.10.1, 5.10.4.3, 5.13.1.4, 5.13.3, 5.13.4.3, 5.7.1.1	1.2.1	SC-7(5)
4	4.6	Securely Manage Enterprise Assets and Software	1	Secure Configuration Management Policy	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) 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.	5.13.1.1		
4	4.7	Manage Default Accounts on Enterprise Assets and Software	1	Secure Configuration Management Policy	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.	5.4.3, 5.6.3.2	2.2.2, 2.3.1	
4	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	2	Secure Configuration Management Policy	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	5.4.3, 5.7.1.1	1.2.5, 2.2.4, 6.4.1	

4	4.10	Enforce Automatic Device Lockout on Portable End-User Devices	2	Secure Configuration Management Policy	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.	5.13.2, 5.5.3	8.3.4	
4	4.11	Enforce Remote Wipe Capability on Portable End-User Devices	2	Secure Configuration Management Policy	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.	5.13.2, 5.13.7.2.1, 5.13.7.3		
4	4.12	Separate Enterprise Workspaces on Mobile End-User Devices	3	Secure Configuration Management Policy	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.	5.13.2, 5.13.6		AC-19(5), SC-39
5	5.1	Establish and Maintain an Inventory of Accounts	1	Account Credential Management Policy	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service 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.	5.4, 5.5.1, 5.6.1, 5.6.3.1	12.5.2	
5	5.2	Use Unique Passwords	1	Account Credential Management Policy	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.	5.13.7.1, 5.13.7.2.1, 5.6.2.1.1	2.2.2, 8.3.5, 8.3.6, 8.6.3	
5	5.3	Disable Dormant Accounts	1	Account Credential Management Policy	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	5.4, 5.6.3.1	8.3.7	AC-2(3)
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	1	Account Credential Management Policy	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.			AC-6(2), AC-6(5)
5	5.5	Establish and Maintain an Inventory of Service Accounts	2	Account Credential Management Policy	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.	5.5.1	7.2.4, 8.2.7	
5	5.6	Centralize Account Management	2	Account Credential Management Policy	Centralize account management through a directory or identity service.			AC-2(1)
6	6.1	Establish an Access Granting Process	1	Account Credential Management Policy	Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.	5.5.1, 5.6.1, 5.6.3.1, 5.6.3.2	7.2.1, 7.2.3, 8.1, 8.1.1, 8.2.1, 8.2.4	AC-2(1)
6	6.2	Establish an Access Revoking Process	1	Account Credential Management Policy	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.	5.12.2, 5.5.1, 5.6.1, 5.6.3.1, 5.6.3.2	8.2.4, 8.2.5	AC-2(1)
6	6.3	Require MFA for Externally-Exposed Applications	1	Account Credential Management Policy	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.	5.6.2.2.1	8.4.3	
6	6.4	Require MFA for Remote Network Access	1	Account Credential Management Policy	Require MFA for remote network access.	5.13.7.2, 5.5.6, 5.6.2.2.1	2.2.7, 8.4.1	
6	6.5	Require MFA for Administrative Access	1	Account Credential Management Policy	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.	5.6.2.2, 5.6.2.2.1	12.5.2	
6	6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	2	Account Credential Management Policy	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.	5.4	6.3.1, 6.4.1	
6	6.7	Centralize Access Control	2	Account Credential Management Policy	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	5.6.2		AC-2(1)
6	6.8	Define and Maintain Role-Based Access Control	3	Account Credential Management Policy	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.	5.11.2, 5.5.1, 5.5.2, 5.5.2.1, 5.5.2.2, 5.5.2.3, 5.5.2.4	7.1, 7.1.1, 7.2, 7.2.1, 7.2.2, 7.2.4, 7.2.6, 7.3, 7.3.1, 7.3.2, 10.3.1	AC-5, AC-6, AC-6(1), AC-6(7), AU-9(4)
7	7.1	Establish and Maintain a Vulnerability Management Process	1	Vulnerability Management Policy	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.	5.10.4.1, 5.13.4.1	6.3.1, 6.3.3, 11.3	
7	7.2	Establish and Maintain a Remediation Process	1	Vulnerability Management Policy	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	5.13.4.1	6.3.1, 6.4.1	
7	7.3	Perform Automated Operating System Patch Management	1	Vulnerability Management Policy	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	5.10.4.1, 5.13.3, 5.13.4.1		SI-2(2)
7	7.4	Perform Automated Application Patch Management	1	Vulnerability Management Policy	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	5.10.4.1, 5.13.3, 5.13.4.1		SI-2(2)

7	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	2	Vulnerability Management Policy	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.		11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3	
7	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	2	Vulnerability Management Policy	Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.		6.4.1, 11.3.2, 11.3.2.1	
7	7.7	Remediate Detected Vulnerabilities	2	Vulnerability Management Policy	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	5.10.4.1, 5.4.3	11.3.1, 11.3.2, 11.3.2.1	
8	8.1	Establish and Maintain an Audit Log Management Process	1	Audit Log Management Policy	Establish and maintain a documented 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.	5.4.1	10.1, 10.1.1	
8	8.2	Collect Audit Logs	1	Audit Log Management Policy	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	5.4.1, 5.4.1.1	5.3.4, 6.4.1, 6.4.2, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2	AU-7
8	8.3	Ensure Adequate Audit Log Storage	1	Audit Log Management Policy	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	5.4.6	10.6, 10.6.1, 10.6.2, 10.6.3	
8	8.4	Standardize Time Synchronization	2	Audit Log Management Policy	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	5.4.4	9.4.5, 10.2, 10.2.1, 10.2.1.2, 10.2.1.5	AU-7
8	8.5	Collect Detailed Audit Logs	2	Audit Log Management Policy	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.	5.4.1.1.1	1.2.6, 1.4.2	AU-3(1), AU-7
8	8.9	Centralize Audit Logs	2	Audit Log Management Policy	Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations include leveraging a SIEM tool to centralize multiple log sources.		10.3.3	AU-6(3)
8	8.10	Retain Audit Logs	2	Audit Log Management Policy	Retain audit logs across enterprise assets for a minimum of 90 days.	5.4.6, 5.4.7	10.5, 10.5.1	
8	8.11	Conduct Audit Log Reviews	2	Audit Log Management Policy	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.	5.4.1, 5.4.3	10.4.1, 10.4.1.1, 10.4.2, 10.4.3	AU-6(1), AU-7(1)
8	8.12	Collect Service Provider Logs	3	Audit Log Management Policy	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.	5.4.1.1		
9	9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	1	Secure Configuration Management Policy	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.	5.10.4.1, 5.10.4.2		
9	9.2	Use DNS Filtering Services	1	Secure Configuration Management Policy	Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.	5.10.1.3	5.4.1	SI-8
9	9.3	Maintain and Enforce Network-Based URL Filters	2	Secure Configuration Management Policy	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.	5.10.1.3, 5.13.4.3	1.2.6, 1.4.2	
9	9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	2	Secure Configuration Management Policy	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	5.10.4.3	2.2.4	CM-10, CM-11, SC-18
9	9.6	Block Unnecessary File Types	2	Secure Configuration Management Policy	Block unnecessary file types attempting to enter the enterprise's email gateway.	5.10.4.3	1.4.3, 5.4.1	SI-8
9	9.7	Deploy and Maintain Email Server Anti-Malware Protections	3	Secure Configuration Management Policy	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	5.10.4.3	5.4.1	SI-16, SI-8
10	10.1	Deploy and Maintain Anti-Malware Software	1	Malware Defence Policy	Deploy and maintain anti-malware software on all enterprise assets.	5.10.4.2, 5.13.3, 5.13.4.2	5.1.1, 5.2.1, 5.2.2, 5.3.2	
10	10.2	Configure Automatic Anti-Malware Signature Updates	1	Malware Defence Policy	Configure automatic updates for anti-malware signature files on all enterprise assets.	5.10.4.2, 5.13.4.2	5.3.1	
10	10.4	Configure Automatic Anti-Malware Scanning of Removable Media	2	Malware Defence Policy	Configure anti-malware software to automatically scan removable media.	5.10.4.3	5.3.3	
10	10.5	Enable Anti-Exploitation Features	2	Malware Defence Policy	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™.	5.13.2		SI-16
10	10.6	Centrally Manage Anti-Malware Software	2	Malware Defence Policy	Centrally manage anti-malware software.	5.10.1.3, 5.4.1		
10	10.7	Use Behavior-Based Anti-Malware Software	2	Malware Defence Policy	Use behavior-based anti-malware software.	5.13.4	5.3.2	

11	11.3	Protect Recovery Data	1	Data Recovery Policy	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.			CP-9(8), SC-28
11	11.4	Establish and Maintain an Isolated Instance of Recovery Data	1	Data Recovery Policy	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.		9.4.1	CP-6, CP-6(1)
11	11.5	Test Data Recovery	2	Data Recovery Policy	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		9.4.1.1	CP-9(1)
12	12.1	Ensure Network Infrastructure is Up-to-Date	1	Secure Configuration Management Policy	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.	5.10.4.1, 5.4.3		CM-8(1)
12	12.2	Establish and Maintain a Secure Network Architecture	2	Secure Configuration Management Policy	Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations will not solely include documentation, but also policy and design components.	5.10.3.1	1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.4.4, 7.1, 7.2.5.1, 11.4.5	CP-6, CP-7, PL-8
12	12.3	Securely Manage Network Infrastructure	2	Secure Configuration Management Policy	Securely manage network infrastructure. Example implementations include version-controlled Infrastructure-as-Code (IaC), and the use of secure network protocols, such as SSH and HTTPS.	5.13.1.1		CM-6, CM-7, SC-23
12	12.4	Establish and Maintain Architecture Diagram(s)	2	Secure Configuration Management Policy	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.	5.7.1.2	1.2.3	PL-8
12	12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	2	Secure Configuration Management Policy	Centralize network AAA.	5.5.2		AC-2(1)
12	12.6	Use of Secure Network Management and Communication Protocols	2	Secure Configuration Management Policy	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	5.10.1, 5.13.1.1, 5.13.3		SC-23
12	12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	2	Secure Configuration Management Policy	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	5.13.6, 5.13.7.2, 5.13.7.2.1, 5.5.2, 5.5.6		AC-17(1), AC-17(3)
12	12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	3	Secure Configuration Management Policy	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.	5.10.3.1, 5.10.3.2		AC-17(3), SI-7
13	13.1	Centralize Security Event Alerting	2	Audit Log Management Policy	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.	5.10.1.3, 5.10.4.4, 5.4.3	10.7, 10.7.1, 10.7.2, 10.7.3, 11.5	AU-6(1), AU-7, IR-4(1), SI-4(2), SI-4(5)
13	13.2	Deploy a Host-Based Intrusion Detection Solution	2		Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	5.10.1.3	6.4.2	
13	13.3	Deploy a Network Intrusion Detection Solution	2		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.	5.10.1.3	11.5.1, 12.10.5	SI-4(4)
13	13.4	Perform Traffic Filtering Between Network Segments	2		Perform traffic filtering between network segments, where appropriate.	5.10.1, 5.4.3, 5.7.1.1	1.3.1, 1.3.2, 1.4.2	
13	13.5	Manage Access Control for Remote Assets	2		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.	5.10.1.1, 5.13.1.2.1, 5.4.3, 5.5.6, 5.6.4	8.4.3	AC-17(1)
13	13.6	Collect Network Traffic Flow Logs	2		Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	5.10.1.3, 5.4.1.1		SI-4(4)
13	13.8	Deploy a Network Intrusion Prevention Solution	3		Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.		6.4.2, 11.5.1, 12.10.5	SI-4(4)
13	13.9	Deploy Port-Level Access Control	3		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.	5.10.1, 5.10.1.1, 5.13.1.1, 5.13.7.2.1, 5.13.7.3	1.2.1, 1.2.5, 1.2.6, 2.2.4	
13	13.10	Perform Application Layer Filtering	3		Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	5.10.1.1, 5.10.3.2, 5.10.4.3, 5.4.3	1.2.1, 1.2.5, 1.2.6	SC-7(8)
13	13.11	Tune Security Event Alerting Thresholds	3		Tune security event alerting thresholds monthly, or more frequently.	5.4.3	12.10.5	
14	14.1	Establish and Maintain a Security Awareness Program	1	Security Awareness Training Policy	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.	5.2.1.1, 5.2.1.2, 5.2.1.3, 5.2.1.4	12.6, 12.6.1, 12.6.2, 12.6.3, 12.6.3.2	
14	14.2	Train Workforce Members to Recognize Social Engineering Attacks	1	Security Awareness Training Policy	Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.	5.2.1.2	12.6.3.1	AT-2(3)

14	14.3	Train Workforce Members on Authentication Best Practices	1	Security Awareness Training Policy	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	5.2.1.3	8.3.8	
14	14.4	Train Workforce on Data Handling Best Practices	1	Security Awareness Training Policy	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.	5.2.1.2, 5.2.1.3		
14	14.5	Train Workforce Members on Causes of Unintentional Data Exposure	1	Security Awareness Training Policy	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.	5.2.1.3		
14	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	1	Security Awareness Training Policy	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	5.2.1.1, 5.3.3		
14	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	1	Security Awareness Training Policy	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.	5.2.1.4		
14	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	1	Security Awareness Training Policy	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.	5.2.1.3	12.6.3.2	
14	14.9	Conduct Role-Specific Security Awareness and Skills Training	2	Security Awareness Training Policy	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.		9.5.1, 9.5.1.3, 12.10.4	
15	15.1	Establish and Maintain an Inventory of Service Providers	1		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.	5.4	12.8.1	
15	15.2	Establish and Maintain a Service Provider Management Policy	2		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.	5.1.2, 5.10.1.5, 5.13.1.2.1	12.8	AC-21, SA-9(2), SR-6
15	15.3	Classify Service Providers	2		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.		12.8.5	AC-20(1), AC-20(2)
15	15.4	Ensure Service Provider Contracts Include Security Requirements	2		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.	5.1.1.8, 5.1.2, 5.10.1.5	11.4.7, 12.4.1, 12.8.2, 12.8.5, 12.9, 12.9.1, 12.9.2	SR-6
15	15.5	Assess Service Providers	3		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.	5.10.1.5	12.8.3	AC-20(1), SI-4
15	15.6	Monitor Service Providers	3		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.	5.1.2	8.2.7, 12.4.2, 12.4.2.1, 12.8.4	SR-6
15	15.7	Securely Decommission Service Providers	3		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.	5.1.2.1		
16	16.1	Establish and Maintain a Secure Application Development Process	2		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.		6.1, 6.1.1, 6.2.1, 6.2.4, 6.3.3	

16	16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	2		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.		6.3.1	
16	16.3	Perform Root Cause Analysis on Security Vulnerabilities	2		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.	5.4.3		
16	16.4	Establish and Manage an Inventory of Third-Party Software Components	2		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.	5.4	12.10.1, 12.10.2	
16	16.5	Use Up-to-Date and Trusted Third-Party Software Components	2		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.		6.3.3, 12.3.4	
16	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	2		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.		6.3.1	
16	16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	2		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.	5.7.1.1	2.2.1	
16	16.8	Separate Production and Non-Production Systems	2		Maintain separate environments for production and non-production systems.		6.5.3	
16	16.9	Train Developers in Application Security Concepts and Secure Coding	2		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.		6.2.2	
16	16.10	Apply Secure Design Principles in Application Architectures	2		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.		2.2.2, 6.2.1	PL-8
16	16.11	Leverage Vetted Modules or Services for Application Security Components	2		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.		6.2.1	SA-15
16	16.12	Implement Code-Level Security Checks	3		Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.		6.2.3, 6.2.3.1	SA-11, SA-15
16	16.13	Conduct Application Penetration Testing	3		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.		6.2.4	

16	16.14	Conduct Threat Modeling	3		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.		12.3.2	
17	17.1	Designate Personnel to Manage Incident Handling	1	Incident Response Management Policy	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, service providers, or a hybrid approach. If using a service provider, 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.	5.3.2	12.10.3, 12.10.4	
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	1	Incident Response Management Policy	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service 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.	5.3.1, 5.3.1.1.1, 5.3.1.1.2		IR-6(3)
17	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	1	Incident Response Management Policy	Establish and maintain an documented 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.	5.10.4.4, 5.2.1.1	12.1	IR-6(1)
17	17.4	Establish and Maintain an Incident Response Process	2	Incident Response Management Policy	Establish and maintain a documented 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.	5.13.5, 5.3.2, 5.3.2.1, 5.3.2.2, 5.3.4	12.10.1, 12.10.2	IR-6, IR-6(1)
17	17.5	Assign Key Roles and Responsibilities	2	Incident Response Management Policy	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	5.3.2	12.10.3	
17	17.6	Define Mechanisms for Communicating During Incident Response	2	Incident Response Management Policy	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification 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.	5.3.1		CP-8, IR-8
17	17.7	Conduct Routine Incident Response Exercises	2	Incident Response Management Policy	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.	5.3.3		IR-3
17	17.8	Conduct Post-Incident Reviews	2	Incident Response Management Policy	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	5.3.2.1	12.10.6	
17	17.9	Establish and Maintain Security Incident Thresholds	3	Incident Response Management Policy	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.	5.3.2	12.10.5	
18	18.1	Establish and Maintain a Penetration Testing Program	2		Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (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.		11.1, 11.1.1, 11.4, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6	
18	18.2	Perform Periodic External Penetration Tests	2		Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.		11.4.3	
18	18.3	Remediate Penetration Test Findings	2		Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.		11.4.4	
18	18.5	Perform Periodic Internal Penetration Tests	3		Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.		11.4.2	