CIS Controls Detailed Breakdown

Learn Where NNT Can Address the 20 CIS Controls

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

CIS CONTROLS 1 - 20 BREAKDOWN

NNT has broken down each of the CIS Controls to show where NNT products can address almost all of the security controls across the 20 categories.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
Control 1: Inventory and Control of Hardware Assets							
■	NNT Vulnerability Tracker and NNT Change Tracker can provide direct asset discovery and tracking of new / changed / removed devices. Change Tracker will also integrate with ITSM systems such as ServiceNow, Remedy or Cherwell to leverage CMDB information as an asset inventory source.	1	1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
■		1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
■		1	1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
■		1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
■		1	1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
■		1	1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
■	NNT Change Tracker: Ports monitored and hardened based on recommended best practice.	1	1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
■	NNT Vulnerability Tracker audits certificate validity.	1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 2: Inventory and Control of Software Assets							
■	NNT Change Tracker will track installed software and updates to expose any additions/changes/removals, and identify any drift from the Authorized Software list. NNT Vulnerability Tracker will identify missing / recommended patches and version updates to software products.	2	2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
■		2	2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
■		2	2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
■		2	2.4	Applications	Identify	Use a Passive Asset Discovery Tool	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
■		2	2.5	Applications	Indentify	Use DHCP Logging to Update Asset Inventory	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
■		2	2.6	Applications	Respond	Maintain Detailed Asset Inventory	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
■	NNT FAST Cloud provides intervention less validation of whitelisted files which may be preferred to process blocking technology.	2	2.7	Applications	Protect	Maintain Asset Inventory Information	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
■		2	2.8	Applications	Protect	Address Unauthorized Assets	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.
■		2	2.9	Applications	Protect	Deploy Port Level Access Control	"The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system."
■		2	2.10	Applications	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 3: Continuous Vulnerability Management							
■	Vulnerability Tracker Standard Functionality - NNT VT is provided with a 'live feed' of new vulnerabilities identified and relevant tests to expose the existence within the network. Any vulnerabilities identified are reported with full background and remediation guidance.	3	3.1	Applica-tions	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
■		3	3.2	Applica-tions	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
■		3	3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
■	WSUS for Windows / Puppet for Linux ++	3	3.4	Applica-tions	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
■		3	3.5	Applica-tions	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
■	NNT Vulnerability Tracker Standard Functionality	3	3.6	Applica-tions	Respond	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
■		3	3.7	Applica-tions	Respond	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 4: Controlled Use of Administrative Privileges							
■	NNT Change Tracker will audit all systems for compliance with secure configuration guidance provided by the Center for Internet Security. NNT are a Certified CIS Vendor.	4	4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
■		4	4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
■		4	4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
■		4	4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
■		4	4.5	Users	Protect	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
■	Specific Independent Control	4	4.6	Users	Protect	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
■	NNT Change Tracker will audit all systems for compliance with secure configuration guidance provided by the Center for Internet Security. NNT are a Certified CIS Vendor.	4	4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
■		4	4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to
■		4	4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers							
■	NNT Change Tracker will audit all systems for compliance with secure configuration guidance provided by the Center for Internet Security. NNT are a Certified CIS Vendor.	5	5.1	Applica-tions	Protect	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.
■		5	5.2	Applica-tions	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
■		5	5.3	Applica-tions	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
■		5	5.4	Applica-tions	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
■		5	5.5	Applica-tions	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.
CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs							
■	NNT Change Tracker will audit all systems for compliance with secure configuration guidance provided by the Center for Internet Security. NNT are a Certified CIS Vendor.	6	6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
■		6	6.2	Network	Detect	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.
■		6	6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
■		6	6.4	Network	Detect	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
■	NNT Log Tracker Standard Functionality - Log Tracker is a full featured SIEM system with a powerful correlation engine	6	6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
■		6	6.6	Network	Detect	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
■		6	6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
■		6	6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 7: Email and Web Browser Protections							
■	Software Baseline report identifies any misalignment with Corporate Standard	7	7.1	Applica-tions	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
■	NNT Change Tracker: CIS Benchmark guidance	7	7.2	Applica-tions	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
■		7	7.3	Applica-tions	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
■		7	7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
		7	7.5	Network	Protect	Subscribe to URL-Categorization service	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
		7	7.6	Network	Detect	Log all URL requests	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
		7	7.7	Network	Protect	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.
		7	7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.
■	NNT Change Tracker: CIS Benchmark guidance	7	7.9	Network	Protect	Block Unnecessary File Types	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.
■		7	7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 8: Malware Defenses							
		8	8.1	Devices	Protect	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
		8	8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
■	NNT Change Tracker: CIS Benchmark guidance	8	8.3	Devices	Protect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
		8	8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
■	NNT Change Tracker: CIS Benchmark guidance	8	8.5	Devices	Protect	Configure Devices Not To Auto-run Content	Configure devices to not auto-run content from removable media.
		8	8.6	Devices	Detect	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
■	NNT Change Tracker: CIS Benchmark guidance	8	8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
■		8	8.8	Devices	Detect	Enable Command-line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services							
■	NNT Change Tracker: Network Port Tracker	9	9.1	Devices	Identify	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.
■		9	9.2	Devices	Protect	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.
■		9	9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.
		9	9.4	Devices	Protect	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
		9	9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 10: Data Recovery Capabilities							
		10	10.1	Data	Protect	Ensure Regular Automated Back Ups	Ensure that all system data is automatically backed up on regular basis.
		10	10.2	Data	Protect	Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
		10	10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
		10	10.4	Data	Protect	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
		10	10.5	Data	Protect	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches							
■	NNT Change Tracker: Configuration standards for all network devices will be enforced	11	11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.
■	NNT Change Tracker: Baseline Report	11	11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.
■	NNT Change Tracker: CIS Benchmark guidance	11	11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.
■	NNT Change Tracker: Firmware/Software versions for network devices validated by Baseline Report	11	11.4	Network	Protect	Install the Latest Stable Version of Any Security-related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.
		11	11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
		11	11.6	Network	Protect	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
		11	11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.
CIS Control 12: Boundary Defense							
■	NNT Vulnerability Tracker and NNT Change Tracker, note that integration with an ITSM CMDB is also being introduced	12	12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.
■		12	12.2	Network	Detect	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.
		12	12.3	Network	Protect	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.
■	NNT Change Tracker: Network Port Tracker	12	12.4	Network	Protect	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.
		12	12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.
		12	12.6	Network	Detect	Deploy Network-based IDS Sensor	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.
		12	12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.
		12	12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.
		12	12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
		12	12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
■	NNT Change Tracker: Configuration standards for all network devices will be enforced	12	12.11	Network	Protect	Require All Remote Login to Use Multi-factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.
		12	12.12	Network	Protect	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.
CIS Control 13: Data Protection							
		13	13.1	Data	Identify	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.
		13	13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
		13	13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
		13	13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.
		13	13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.
■	NNT Change Tracker: Configuration standards for all network devices will be enforced ie BitLocker rules	13	13.6	Data	Protect	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.
		13	13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
■	NNT Change Tracker: Configuration standards for all network devices will be enforced ie disable removable storage	13	13.8	Data	Protect	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.
■	NNT Change Tracker: Configuration standards for all network devices will be enforced ie BitLocker rules	13	13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.
CIS Control 14: Controlled Access Based on Need to Know							
		14	14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).
		14	14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.
		14	14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.
		14	14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.
		14	14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.
		14	14.6	Data	Protect	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
		14	14.7	Data	Protect	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.
		14	14.8	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
■	NNT Change Tracker: Audit Policy standards will be enforced by CT scans	14	14.9	Data	Protect	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.
CIS Control 15: Wireless Access Control							
		15	15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.
■	NNT Vulnerability Tracker Standard Functionality	15	15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.
		15	15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.
■	NNT Change Tracker: CIS Benchmark guidance	15	15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.
■		15	15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.
■		15	15.6	Devices	Protect	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.
■		15	15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
■		15	15.8	Network	Protect	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.
■		15	15.9	Devices	Protect	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
		15	15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 16: Account Monitoring and Control							
		16	16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.
■	NNT Change Tracker: Configuration standards for all devices will be enforced	16	16.2	Users	Protect	Configure Central-ized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.
		16	16.3	Users	Protect	Require Multi-factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.
		16	16.4	Users	Protect	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.
■	NNT Change Tracker: Configuration standards for all devices will be enforced	16	16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
■		16	16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.
		16	16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.
		16	16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.
■	NNT Change Tracker: Configuration standards for all devices will be enforced	16	16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.
■		16	16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.
■		16	16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.
■		16	16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.
■		16	16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
CIS Control 17: Implement a Security Awareness and Training Program							
		17	17.1			Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.
		17	17.2			Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.
		17	17.3			Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
		17	17.4			Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
		17	17.5			Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
		17	17.6			Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
		17	17.7			Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.
		17	17.8			Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
CIS Control 18: Application Software Security							
		18	18.1			Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.
		18	18.2			Ensure Explicit Error Checking is Performed for All In-house Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
■	NNT Change Tracker: Firmware/Software versions for network devices validated by Baseline Report	18	18.3			Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.
■		18	18.4			Only Use Up-to-date And Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
		18	18.5			Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.
		18	18.6			Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
		18	18.7			Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.
		18	18.8			Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.
		18	18.9			Separate Production and Non-Production Systems	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.
		18	18.10			Deploy Web Application Firewalls (WAFs)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
■	NNT Change Tracker: Configuration standards for all devices will be enforced	18	18.11			Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.
CIS Control 19: Incident Response and Management							
		19	19.1			Document Incident Response Procedures	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.
		19	19.2			Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.
		19	19.3			Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
		19	19.4			Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
		19	19.5			Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.
		19	19.6			Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
		19	19.7			Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.
		19	19.7			Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.
		19	19.8			Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.
CIS Control 20: Penetration Tests and Red Team Exercises							
■	NNT Vulnerability Tracker Standard Functionality	20	20.1			Establish a Penetration Testing Program	Establish secure coding practices appropriate to the programming language and development environment being used.
■		20	20.2			Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
		20	20.3			Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

Map	NNT Description	CIS Control	CIS Sub-control	Asset Type	Security Function	Title	Description
		20	20.4			Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
		20	20.5			Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.
■	NNT Vulnerability Tracker Standard Functionality	20	20.6			Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
■		20	20.7			Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
		20	20.8			Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they're only being used for legitimate purposes, and are removed or restored to normal function after testing is over.