APPENDIX D

MAPPING TABLES

MAPPING CUI SECURITY REQUIREMENTS TO SECURITY CONTROLS

Tables D-1 through D-14 provide an informal mapping of the CUI security requirements to the relevant security controls in NIST Special Publication 800-53. The mapping tables are included for informational purposes only and are not intended to convey or impart any additional CUI security requirements beyond those requirements defined in Chapter Three. Moreover, because the security controls were developed for federal agencies, the supplemental guidance associated with those controls may not be applicable to nonfederal organizations. In some cases, the relevant security controls include additional expectations beyond those required to protect CUI and have been tailored using the criteria in Chapter Two. Only the portion of the security control relevant to the CUI security requirement is applicable. The tables also include a secondary mapping of the security controls from Special Publication 800-53 to the relevant controls in ISO/IEC 27001, Annex A. The NIST to ISO/IEC mapping is obtained from Special Publication 800-53, Appendix H. An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control. It is also important to note that, due to the tailoring for CUI, satisfaction of a basic or derived security requirement does *not* mean that the corresponding security control or control enhancement from NIST Special Publication 800-53 has been met, since certain elements of the control or control enhancement that are not essential to protecting the confidentiality of CUI are not reflected in those requirements.

Organizations that have implemented or plan to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity* can use the mapping of the CUI security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001 to locate the equivalent controls in the categories and subcategories associated with the core functions of the Framework: identify, protect, detect, respond, and recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the CUI security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

Table D-1: Mapping Access Control Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
Derived Security Requirements				
3.1.3 Control the flow of CUI in accordance with approved authorizations.	AC-4	Information Flow Enforcement	A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	A.6.1.2	Segregation of duties
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	A.9.1.2	Access to networks and network services
				A.9.2.3	Management of privileged access rights
				A.9.4.4	Use of privileged utility programs
				A.9.4.5	Access control to program source code
		AC-6(1)	Least Privilege *Authorize Access to Security Functions*	*No direct mapping.*	
		AC-6(5)	Least Privilege *Privileged Accounts*	*No direct mapping.*	
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege *Non-Privileged Access for Nonsecurity Functions*	*No direct mapping.*	
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	*No direct mapping.*	
		AC-6(10)	Least Privilege *Prohibit Non-Privileged Users From Executing Privileged Functions*	*No direct mapping.*	
3.1.8	Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	A.9.4.2	Secure logon procedures
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	A.9.4.2	Secure logon procedures
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	AC-11	Session Lock	A.11.2.8	Unattended user equipment
				A.11.2.9	Clear desk and clear screen policy
		AC-11(1)	Session Lock *Pattern-Hiding Displays*	*No direct mapping.*	
3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12	Session Termination	*No direct mapping.*	
3.1.12	Monitor and control remote access sessions.	AC-17(1)	Remote Access *Automated Monitoring / Control*	*No direct mapping.*	
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access *Protection of Confidentiality / Integrity Using Encryption*	*No direct mapping.*	
3.1.14	Route remote access via managed access control points.	AC-17(3)	Remote Access *Managed Access Control Points*	*No direct mapping.*	

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	Remote Access *Privileged Commands / Access*	*No direct mapping.*	
3.1.16 Authorize wireless access prior to allowing such connections.	AC-18	Wireless Access	A.6.2.1	Mobile device policy
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
3.1.17 Protect wireless access using authentication and encryption.	AC-18(1)	Wireless Access *Authentication and Encryption*	*No direct mapping.*	
3.1.18 Control connection of mobile devices.	AC-19	Access Control for Mobile Devices	A.6.2.1	Mobile device policy
			A.11.2.6	Security of equipment and assets off-premises
			A.13.2.1	Information transfer policies and procedures
3.1.19 Encrypt CUI on mobile devices.	AC-19(5)	Access Control for Mobile Devices *Full Device / Container-Based Encryption*	*No direct mapping.*	
3.1.20 Verify and control/limit connections to and use of external information systems.	AC-20	Use of External Information Systems	A.11.2.6	Security of equipment and assets off-premises
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
	AC-20(1)	Use of External Information Systems *Limits on Authorized Use*	*No direct mapping.*	
3.1.21 Limit use of organizational portable storage devices on external information systems.	AC-20(2)	Use of External Information Systems *Portable Storage Devices*	*No direct mapping.*	
3.1.22 Control information posted or processed on publicly accessible information systems.	AC-22	Publicly Accessible Content	*No direct mapping.*	

Table D-2: Mapping Awareness and Training Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.2 AWARENESS AND TRAINING				
Basic Security Requirements				
3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
			A.12.2.1	Controls against malware
	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.				
Derived Security Requirements				
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	*No direct mapping.*	

Table D-3: Mapping Audit and Accountability Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.3 AUDIT AND ACCOUNTABILITY				
Basic Security Requirements				
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	AU-2	Audit Events	*No direct mapping.*	
	AU-3	Content of Audit Records	A.12.4.1*	Event logging
	AU-3(1)	Content of Audit Records *Additional Audit Information*	*No direct mapping.*	
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	AU-6	Audit Review, Analysis, and Reporting	A.12.4.1	Event logging
			A.16.1.2	Reporting information security events
			A.16.1.4	Assessment of and decision on information security events
	AU-12	Audit Generation	A.12.4.1	Event logging
			A.12.4.3	Administrator and operator logs
Derived Security Requirements				
3.3.3 Review and update audited events.	AU-2(3)	Audit Events *Reviews and Updates*	*No direct mapping.*	
3.3.4 Alert in the event of an audit process failure.	AU-5	Response to Audit Processing Failures	*No direct mapping.*	
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(3)	Audit Review, Analysis, and Reporting *Correlate Audit Repositories*	*No direct mapping.*	
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7	Audit Reduction and Report Generation	*No direct mapping.*	
3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU-8	Time Stamps	A.12.4.4	Clock synchronization
	AU-8(1)	Time Stamps *Synchronization With Authoritative Time Source*	*No direct mapping.*	
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9	Protection of Audit Information	A.12.4.2	Protection of log information
			A.12.4.3	Administrator and operator logs
			A.18.1.3	Protection of records

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*
3.3.9	Limit management of audit functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information *Access by Subset of Privileged Users*	*No direct mapping.*

Table D-4: Mapping Configuration Management Requirements to Security Controls[27]

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.4 CONFIGURATION MANAGEMENT				
Basic Security Requirements				
3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. **3.4.2** Establish and enforce security configuration settings for information technology products employed in organizational information systems.	CM-2	Baseline Configuration	*No direct mapping.*	
	CM-6	Configuration Settings	*No direct mapping.*	
	CM-8	Information System Component Inventory	A.8.1.1	Inventory of assets
			A.8.1.2	Ownership of assets
	CM-8(1)	Information System Component Inventory *Updates During Installations / Removals*	*No direct mapping.*	
Derived Security Requirements				
3.4.3 Track, review, approve/disapprove, and audit changes to information systems.	CM-3	Configuration Change Control	A.12.1.2	Change management
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.14.2.4	Restrictions on changes to software packages
3.4.4 Analyze the security impact of changes prior to implementation.	CM-4	Security Impact Analysis	A.14.2.3	Technical review of applications after operating platform changes
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	CM-5	Access Restrictions for Change	A.9.2.3	Management of privileged access rights
			A.9.4.5	Access control to program source code
			A.12.1.2	Change management
			A.12.1.4	Separation of development, testing, and operational environments
			A.12.5.1	Installation of software on operational systems

[27] CM-7(5), a least functionality whitelisting policy, is listed as an alternative to CM-7(4), the least functionality blacklisting policy, for organizations desiring greater protection for information systems containing CUI. CM-7(5) is only required in federal information systems at the high security control baseline in accordance with NIST Special Publication 800-53.

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	CM-7	Least Functionality	A.12.5.1*	Installation of software on operational systems
3.4.7 Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.	CM-7(1)	Least Functionality *Periodic Review*	*No direct mapping.*	
	CM-7(2)	Least Functionality *Prevent program execution*	*No direct mapping.*	
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	CM-7(4)	Least Functionality *Unauthorized Software/ Blacklisting*	*No direct mapping.*	
	CM-7(5)	Least Functionality *Authorized Software/ Whitelisting*	*No direct mapping.*	
3.4.9 Control and monitor user-installed software.	CM-11	User-Installed Software	A.12.5.1	Installation of software on operational systems
			A.12.6.2	Restrictions on software installation

Table D-5: Mapping Identification and Authentication Requirements to Security Controls[28]

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5 IDENTIFICATION AND AUTHENTICATION				
Basic Security Requirements				
3.5.1 Identify information system users, processes acting on behalf of users, or devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
			A.9.2.4	Management of secret authentication information of users
			A.9.3.1	Use of secret authentication information
			A.9.4.3	Password management system
Derived Security Requirements				
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts*	*No direct mapping.*	
	IA-2(2)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts*	*No direct mapping.*	
	IA-2(3)	Identification and Authentication (Organizational Users) *Local Access to Privileged Accounts*	*No direct mapping.*	
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts-Replay Resistant*	*No direct mapping.*	
	IA-2(9)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts-Replay Resistant*	*No direct mapping.*	
3.5.5 Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration

[28] IA-2(9) is *not* currently in the NIST Special Publication 800-53 moderate security control baseline although it will be added to the baseline in the next update. Employing multifactor authentication without a replay-resistant capability for non-privileged accounts creates a significant vulnerability for information systems transmitting CUI.

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5.6	Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management *Password-Based Authentication*	*No direct mapping.*	
3.5.8	Prohibit password reuse for a specified number of generations.				
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.				
3.5.10	Store and transmit only encrypted representation of passwords.				
3.5.11	Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure logon procedures

Table D-6: Mapping Incident Response Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.6 INCIDENT RESPONSE				
Basic Security Requirements				
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. **3.6.2** Track, document, and report incidents to appropriate organizational officials and/or authorities.	IR-2	Incident Response Training	A.7.2.2*	Information security awareness, education, and training
	IR-4	Incident Handling	A.16.1.4	Assessment of and decision on information security events
			A.16.1.5	Response to information security incidents
			A.16.1.6	Learning from information security incidents
	IR-5	Incident Monitoring	*No direct mapping.*	
	IR-6	Incident Reporting	A.6.1.3	Contact with authorities
			A.16.1.2	Reporting information security events
	IR-7	Incident Response Assistance	*No direct mapping.*	
Derived Security Requirements				
3.6.3 Test the organizational incident response capability.	IR-3	Incident Response Testing	*No direct mapping.*	
	IR-3(2)	Incident Response Testing *Coordination with Related Plans*	*No direct mapping.*	

Table D-7: Mapping Maintenance Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.7 MAINTENANCE				
Basic Security Requirements				
3.7.1 Perform maintenance on organizational information systems. **3.7.2** Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
	MA-3	Maintenance Tools	*No direct mapping.*	
	MA-3(1)	Maintenance Tools *Inspect Tools*	*No direct mapping.*	
	MA-3(2)	Maintenance Tools *Inspect media*	*No direct mapping.*	
Derived Security Requirements				
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	MA-3(2)	Maintenance Tools	*No direct mapping.*	
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	*No direct mapping.*	
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	*No direct mapping.*	

Table D-8: Mapping Media Protection Requirements to Security Controls[29]

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8 MEDIA PROTECTION				
Basic Security Requirements				
3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. **3.8.2** Limit access to CUI on information system media to authorized users. **3.8.3** Sanitize or destroy information system media containing CUI before disposal or release for reuse.	MP-2	Media Access	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
	MP-4	Media Storage	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
	MP-6	Media Sanitization	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.2	Disposal of media
			A.11.2.7	Secure disposal or reuse of equipment
Derived Security Requirements				
3.8.4 Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	A.8.2.2	Labelling of Information
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.3	Physical media transfer
			A.11.2.5	Removal of assets
			A.11.2.6	Security of equipment and assets off-premises
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport *Cryptographic Protection*	*No direct mapping.*	
3.8.7 Control the use of removable media on information system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media

[29] CP-9, *Information System Backup*, is included with the Media Protection family since the Contingency Planning family was not included in the CUI security requirements.

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use *Prohibit Use Without Owner*	*No direct mapping.*	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	Information System Backup	A.12.3.1	Information backup
				A.17.1.2	Implementing information security continuity
				A.18.1.3	Protection of records

Table D-9: Mapping Personnel Security Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.9 PERSONNEL SECURITY				
Basic Security Requirements				
3.9.1 Screen individuals prior to authorizing access to information systems containing CUI. **3.9.2** Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS-3	Personnel Screening	A.7.1.1	Screening
	PS-4	Personnel Termination	A.7.3.1	Termination or change of employment responsibilities
			A.8.1.4	Return of assets
	PS-5	Personnel Transfer	A.7.3.1	Termination or change of employment responsibilities
			A.8.1.4	Return of assets
Derived Security Requirements	None.			

Table D-10: Mapping Physical Protection Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.10 PHYSICAL PROTECTION				
Basic Security Requirements				
3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. **3.10.2** Protect and monitor the physical facility and support infrastructure for those information systems.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
	PE-5	Access Control for Output Devices	A.11.1.2	Physical entry controls
			A.11.1.3	Securing offices, rooms, and facilities
	PE-6	Monitoring Physical Access	*No direct mapping.*	
Derived Security Requirements				
3.10.3 Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	A.11.1.1	Physical security perimeter
			A.11.1.2	Physical entry controls
3.10.4 Maintain audit logs of physical access.			A.11.1.3	Securing offices, rooms, and facilities
3.10.5 Control and manage physical access devices.				
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	PE-17	Alternate Work Site	A.6.2.2	Teleworking
			A.11.2.6	Security of equipment and assets off-premises
			A.13.2.1	Information transfer policies and procedures

Table D-11: Mapping Risk Assessment Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.11 RISK ASSESSMENT				
Basic Security Requirements				
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
Derived Security Requirements				
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
	RA-5(5)	Vulnerability Scanning *Privileged Access*	*No direct mapping.*	
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

Table D-12: Mapping Security Assessment Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.12 SECURITY ASSESSMENT				
Basic Security Requirements				
3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	CA-2	Security Assessments	A.14.2.8	System security testing
			A.18.2.2	Compliance with security policies and standards
			A.18.2.3	Technical compliance review
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	CA-5	Plan of Action and Milestones	*No direct mapping.*	
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	CA-7	Continuous Monitoring	*No direct mapping.*	
Derived Security Requirements	None.			

Table D-13: Mapping System and Communications Protection Requirements to Security Controls[30]

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION				
Basic Security Requirements				
3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	SA-8	Security Engineering Principles	A.14.2.5	Secure system engineering principles
Derived Security Requirements				
3.13.3 Separate user functionality from information system management functionality (e.g., privileged user functions).	SC-2	Application Partitioning	*No direct mapping.*	
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Information In Shared Resources	*No direct mapping.*	
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5)	Boundary Protection *Deny By Default / Allow By Exception*	*No direct mapping.*	

[30] SA-8, *Security Engineering Principles*, is included with the System and Communications Protection family since the System and Services Acquisition family was not included in the CUI security requirements.

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	SC-7(7)	Boundary Protection *Prevent Split Tunneling for Remote Devices*	*No direct mapping.*	
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8	Transmission Confidentiality and Integrity	A.8.2.3	Handling of Assets
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.13.2.3	Electronic messaging
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
	SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*	*No direct mapping.*	
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	A.13.1.1	Network controls
3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system.	SC-12	Cryptographic Key Establishment and Management	A.10.1.2	Key Management
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection	A.10.1.1	Policy on the use of cryptographic controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.5	Regulation of cryptographic controls
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	SC-15	Collaborative Computing Devices	A.13.2.1*	Information transfer policies and procedures

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13.13	Control and monitor the use of mobile code.	SC-18	Mobile Code	*No direct mapping.*	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	Voice over Internet Protocol	*No direct mapping.*	
3.13.15	Protect the authenticity of communications sessions.	SC-23	Session Authenticity	*No direct mapping.*	
3.13.16	Protect the confidentiality of CUI at rest.	SC-28	Protection of Information at Rest	A.8.2.3*	Handling of Assets

Table D-14: Mapping System and Information Integrity Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.14 SYSTEM AND INFORMATION INTEGRITY				
Basic Security Requirements				
3.14.1 Identify, report, and correct information and information system flaws in a timely manner. **3.14.2** Provide protection from malicious code at appropriate locations within organizational information systems. **3.14.3** Monitor information system security alerts and advisories and take appropriate actions in response.	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.16.1.3	Reporting information security weaknesses
	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups
Derived Security Requirements				
3.14.4 Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.				
3.14.6 Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	Information System Monitoring	*No direct mapping.*	
	SI-4(4)	Information System Monitoring *Inbound and Outbound Communications Traffic*	*No direct mapping.*	
3.14.7 Identify unauthorized use of the information system.	SI-4	Information System Monitoring	*No direct mapping.*	