An Introduction to NIST Special Publication 800-171 for Higher Education Institutions

A Higher Education Information Security Council (HEISC) Resource

October 2016

Higher Education Information Security Council

What Is NIST 800-171?

The National Institute of Standards and Technology (NIST) published *Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* in June 2015 (updated January 21, 2016). The purpose of this NIST publication is to provide guidance for federal agencies to ensure that certain types of federal information is protected when processed, stored, and used in non-federal information systems.

NIST 800-171 applies to Controlled Unclassified Information (also called CUI, described more fully later in this guide) shared *by* the federal government *with* a nonfederal entity. In the higher education context, the federal government often shares data with institutions for research purposes or in carrying out the work of federal agencies. In many of those instances, other federal laws or regulations might address how that information must be protected (e.g., FISMA). In some cases, however, there may not be a law that specifically addresses how the CUI data received from the federal government must be protected. In those instances, NIST 800-171 will apply when the federal government shares controlled unclassified information with higher education institutions. As such, the controls specified in NIST 800-171 will need to be addressed in those higher education institutional IT systems that store CUI.

The controls specified in NIST 800-171 are based on NIST *Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*.[1] The controls were tailored from NIST 800-53 specifically to protect CUI in nonfederal IT systems from unauthorized disclosure. There are 14 families of security requirements outlined in NIST 800-171, comprising 109 individual controls. The families are:[2]

- *Access control:* generally limits system access to authorized users
- *Awareness and training:* generally alerts employees to information security risks
- *Audit and accountability:* involves the creation, protection, retention, and review of system logs
- *Configuration management:* involves creation of baseline configurations and use of robust change management processes
- *Identification and authentication:* involves central authentication and multi-factor for local and network access to resources
- *Incident response:* involves developing operations to prepare for, detect, analyze, contain, recover from, and respond to incidents affecting information
- *Maintenance:* involves maintenance of systems

[1] Note that FISMA compliance typically requires an Authority to Operate (ATO), which is a government agency issued letter providing authorization to operate any information systems used to support a contract. This is not likely to be required under NIST 800-171.

[2] This document contains an appendix that maps NIST 800-171 controls against NIST 800-53, ISO 27002:2013, and the 20 Critical Controls.

- *Media protection:* involves the sanitization and destruction of media containing CUI
- *Personnel security:* involves screening individuals before granting them access to information systems with CUI
- *Physical protection:* involves limiting physical access to systems to only authorized individuals
- *Risk assessment:* involves assessing the operational risk associated with processing, storage, and transmission of CUI
- *Security assessment:* involves assessing effectiveness of security controls and addressing deficiencies to limit vulnerabilities
- *System and communications protection:* involves use of secure design principles in system architecture and software development life cycle
- *System and information security:* involves monitoring for an alerting on system flaws and vulnerabilities

What Is Controlled Unclassified Information (CUI)?

U.S. government information classifications have been well defined when dealing with classified (or national security) information. An information security professional in today's higher education realm may not have had an opportunity to interact with systems dealing with government classified information unless he or she has served in the U.S. military or worked for a federal agency. Stated simply, there are two effective realms pertinent to the CUI context:

- Classified[3]
- Unclassified

Until recently, the unclassified realm contained various subcategories and definitions that were instituted by numerous federal agencies. These information categories were an attempt to identify information, mostly paper-based, that required additional protection from disclosure, but not to the level of classified information,[4] and each federal agency applied different control requirements for their particular definition of unclassified information. In 2010, the White House issued Executive Order 13556, which defined Controlled Unclassified Information (CUI)[5] to gather these various information categories into a single definition for all federal agencies, placing the National Archives in the role of creating the definitions. These can be found in the Controlled Unclassified Information (CUI) Registry.[6]

[3] Classified information labels include *Top Secret/SCI, Top Secret, Secret,* and *Confidential*. The various types of classified information are outside the scope of this guide. For more information generally, see *Frequently Asked Questions on Identifying and Handling Classified Records in Private Papers*.

[4] Some labels used to specify this type of unclassified information included *For Official Use Only/FOUO* or *Sensitive But Unclassified/SBU.*

[5] See *What Is CUI? Answers to the Most Frequently Asked Questions*.

[6] The National Archives promulgated a rule for how the federal agencies must designate, safeguard, disseminate, mark, decontrol, and dispose of CUI in September 2016.

In summary, CUI can describe any information that is not in the *classified* category. Its use was originally intended for federal agencies to manage their own complex world of nonclassified information. However, as federal agencies look to vendors and service providers for cost-effective support, they are obligated under FISMA to address security of information that is in the possession of its vendors and contractors. In this context, one can easily envision that leadership in federal agencies may attempt to use CUI to claim "ownership" of information they deem pertinent to their missions that is owned or under the stewardship of higher education institutions. Colleges and universities often produce knowledge—and disseminate information via publications—that overlaps with what federal agencies produce for public consumption. The most obvious application of CUI is for research conducted under federally funded contracts (often referred to as "grants").

Common types of data in higher education that "may" be called CUI.

A higher education institution must review its contracts with federal agencies carefully. In order for NIST 800-171 to apply to higher education institutions, data received from the federal government must be designated as CUI and there must be a document (contract) referencing both (1) the data specifically identified as CUI and received from the federal government, and (2) that the institution must follow the terms of NIST 800-171.

There are 22 approved CUI categories,[7] most of which may easily be found in higher education, including agriculture, copyright, critical infrastructure, export control, financial, information systems vulnerability information, legal, patent, statistical, and various privacy-related data.

Here are some detailed examples of controlled unclassified information **that a higher education institution might *receive* from** (or produce under contract for) a federal agency:

1. Student records or personally identifiable information (PII)
2. Export control–research data
3. Critical infrastructure information
4. Controlled technical information

What institutional information should be "out of scope"?

Institutional information that is not under a contractual obligation is out of scope. The only institutional information that is in scope for CUI controls via the application of NIST 800-171 is that which is agreed upon through a contract between the federal agency and the institution.[8] Usually this comes in the context of information being shared with an institution under that

[7] Slide 8 of the Information Security Oversight Office (ISOO) presentation, "Controlled Unclassified Information: Executive Order 13556," provides an overview of the 22 approved CUI categories.

[8] Note that DFARS (Department of Defense Federal Acquisition Regulations) has a clause that specifies the use of NIST SP 800-171 controls to protect CUI for all Department of Defense contracts. Other federal agencies do not have a blanket FAR (Federal Acquisition Regulation), so if a contract with a federal agency does not state CUI protections are required to protect data received from the federal agency, then NIST 800-171 cannot be enforced until the next contract revision.

contract. NIST suggests universities be exacting in what is defined as CUI to be protected, ensuring that the CUI is defined in the Controlled Unclassified Information (CUI) registry.

How Are Institutions Responding to NIST 800-171?

Like many information security compliance activities, an institutional response to the requirements of NIST 800-171 will require the involvement of multiple stakeholders. As federal contracts begin to specify the CUI shared by the federal government and require NIST 800-171 compliance, institutions will need to ensure that those persons using such data, and those systems processing such data, are aware of the data-protection requirements specified by NIST 800-171.

This process may take some time. While the Department of Defense has already started to require NIST 800-171 in its contracts, the requirements have not yet been adopted across the federal government in all of its non-defense-related contracts. In addition, where isolating CUI from the campus-computing infrastructure is not possible, an institution must then compare the NIST 800-171 controls with its own already established information security controls. In some cases, it may be that new controls will need to be implemented in campus information systems to protect CUI. In those instances, an institution should be prepared to ask for additional time to comply with NIST 8800-171 via the contractual negotiation process.

The following paragraphs highlight how some institutions are approaching activities that may require NIST 800-171 compliance.

University of Notre Dame

The cost of implementing NIST 800-171 can be prohibitive. For example, Notre Dame maintains a segregated PCI DSS–compliant network for five merchants at a cost of well over $100,000 annually, an environment that is less burdensome to maintain than a NIST 800-171–compliant network. For institutions that may only have a handful of small, regulated research projects, justifying the costs of supporting a fully compliant NIST 800-171 environment may be difficult. To keep costs low, among other reasons, Notre Dame decided to use Amazon GovCloud[9] for its NIST 800-171 infrastructure. Amazon designed GovCloud to host sensitive data with U.S. Government compliance requirements, and it meets the requirements of NIST 800-171. As with all IaaS (Infrastructure as a Service) cloud solutions, GovCloud operates as a shared security model, where Amazon meets many of the infrastructure-level security requirements and provides many of the means for customers to meet other requirements. For example, GovCloud provides infrastructure and services for physical security, disaster recovery, redundant data centers, and network controls, while the customer's obligation is to properly implement or build on these services to meet the requirements not already met by GovCloud. Amazon's pay-

[9] See *AWS GovCloud (US)*.

for-what-you-use model also keeps costs low. For these reasons, Notre Dame is currently building out its NIST 800-171 GovCloud infrastructure based on Amazon’s NIST 800-53 build scripts.

University of Pittsburgh

When tackling FISMA compliance (800-53) in 2012, Pitt chose a similar model to Notre Dame in which it created a FISMA-compliant private cloud in the data center. This model allowed Pitt to quickly onboard research contracts that required FISMA Moderate or Low compliance, without impacting the larger university network and computing environment. The disadvantages of this approach are that it required care and feeding of a duplicative environment and that, in many cases, it restricted the collaboration that is often a requirement of research. However, tackling FISMA compliance with a scope of anything larger than an isolated environment at Pitt would have been difficult. The university’s FISMA-compliance efforts, specifically the 800-53 controls that represent Low compliance, have enable Pitt to apply a broader scope to its 800-171 compliance. Due to FISMA, many 800-53 controls became part of standard operating procedure for the infrastructure and security divisions within the central IT department. When 800-171 came out, a gap analysis conducted by the information security team showed that the university was already accomplishing 85% or more via standard operating procedure (SOP). Pitt is creating a master 800-171 security plan document that details the existing SOP to accomplish compliance and is working on closing identified gaps within the next six months. All of these controls will be tested to ensure a compliant state, after which any system hosted in the network operations center will be 800-171 compliant, as will the university network itself. Lastly, if departments are compliant with workstation management best practice procedures, 800-171 compliance will extend all the way to the end point. While the goal is to use SOP to accomplish 800-171 compliance, the security division will still certify each contract requiring compliance through existing processes in place with the Office of Research (through which all contracts containing security language are reviewed) and determine how it should be hosted.

North Carolina State University

NC State is in the final stages of developing an overall cybersecurity strategic plan with a vision to create an agile, secure, and resilient cyberenvironment that empowers the NC State community to innovate and achieve the university’s mission. Securing research data and intellectual property is a key strategic objective in the plan. Tactically, NC State is approaching this research security problem in a similar manner to Notre Dame and Pittsburgh. The university is building a secure research enclave, seeking to create a secure MPLS zone for research computing and storage on campus in its data centers while also leveraging compliant cloud services such as AWS, Azure, and the like. NC State realizes that its goal of becoming NIST 800-53 Moderate compliant will take a while to accomplish. And research data is not its only concern, so it has adopted the NIST Cybersecurity Framework as its overall umbrella. A high-level perspective of the program will be defined in terms of functional outcomes; peeling back the layers will reveal NIST 800-171 compliance for research, ISO 27001/2 for other areas, and PCI DSS. So as not boil the ocean, NC State is starting with the SANS Top 20 Security Controls and working toward more comprehensive coverage over time, ensuring that the outcome is not just an IT solution but also a partnership between IT and the university research group. The university has leveraged Google Apps for Government to manage some projects and CloudLock to monitor policies and control third-party application access.

Conclusion

Institutions continue to refine their understanding of the impact of NIST Special Publication 800-171 on their IT systems and the data they receive from the federal government. Until the federal government creates additional guidance, the following list summarizes key points:

- NIST 800-171 applies to data that the federal government designates as Controlled Unclassified Information (CUI) when they are shared *by* the federal government *with* a nonfederal entity and *when no other* federal law or regulation (e.g., FISMA) addresses how to protect the underlying data.
- Depending on the type of data received from the federal government, CUI could include data received as part of a research grant or data received to conduct business (e.g., student financial aid information).
- A higher education institution must review its contracts with federal agencies carefully. There must be a document (contract) referencing both (1) the data the federal agency is sharing that it has specifically identified as CUI, and (2) that the institution must follow the terms of NIST 800-171.

Additional Resources

- NIST *Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.
- NIST SP 800-171 Compliance Template created by the Common Solutions Group.
- Virginia Tech's PowerPoint slides, "Controlled Unclassified Information and NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (created by Virginia Tech research and compliance staff T.J. Beckett and John Talerico).
- Hogan Lovells on DFARS extension.
- FSA July 2015 bulletin that mentions 800-171 as an industry best practice.

Appendix: NIST 800-171 Controls, NIST 800-53, ISO 27002:2013, and the 20 Critical Controls

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
Control Family: Access Control				
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC-2, AC-3, AC-17	A.6.2.1, A.6.2.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.2, A.14.1.3, A.18.1.3	12, 13, 15, 16, 17,
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2, AC-3, AC-17	A.6.2.1, A.6.2.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.2, A.14.1.3, A.18.1.3	12, 13, 15, 16, 17
3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC-4	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	10, 11, 13, 17, 19
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	A.6.1.2	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6, AC-6(1), AC-6(5)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	12, 15
3.1.6	Use nonprivileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	12, 15
3.1.7	Prevent nonprivileged users from executing privileged functions and audit the execution of such functions.	AC-6(9), AC-6(10)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	12, 15
3.1.8	Limit unsuccessful logon attempts.	AC-7	A.9.4.2	16
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-9	A.9.4.2	
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	AC-11, AC-11(1)	A.11.2.8, A.11.2.9	16
3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12	None	16
3.1.12	Monitor and control remote access sessions.	AC-17(1)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	12, 13

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	12, 13
3.1.14	Route remote access via managed access control points.	AC-17(3)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	12, 13
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	12, 13
3.1.16	Authorize wireless access prior to allowing such connections.	AC-18	A.6.2.1, A.13.1.1, A.13.2.1	7
3.1.17	Protect wireless access using authentication and encryption.	AC-18(1)	A.6.2.1, A.13.1.1, A.13.2.1	7
3.1.18	Control connection of mobile devices.	AC-19	A.6.2.1, A.11.2.6, A.13.2.1	7, 12
3.1.19	Encrypt CUI on mobile devices.	AC-19(5)	A.6.2.1, A.11.2.6, A.13.2.1	7, 12
3.1.20	Verify and control/limit connections to and use of external information systems.	AC-20, AC-20(1)	A.11.2.6, A.13.1.1, A.13.2.1	13
3.1.21	Limit use of organizational portable storage devices on external information systems.	AC-20(2)	A.11.2.6, A.13.1.1, A.13.2.1	13
3.1.22	Control information posted or processed on publicly accessible information systems.	AC-22	None	
Control Family: Awareness and Training				
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, AT-3	A.7.2.2, A.12.2.1	9
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	AT-2, AT-3	A.7.2.2, A.12.2.1	9
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	A.7.2.2, A.12.2.1	9

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
Control Family: Audit and Accountability				
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, AU-3, AU-3(1), AU-6, AU-12	A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.4	14
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-2, AU-3, AU-3(1), AU-6, AU-12	A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.4	14
3.3.3	Review and update audited events.	AU-2(3)	None	14
3.3.4	Alert in the event of an audit process failure.	AU-5	None	14
3.3.5	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(1), AU-6(3)	A.12.4.1, A.16.1.2, A.16.1.4	14
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7	None	14
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, AU-8(1)	A.12.4.4	14
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9	A.12.4.2, A.12.4.3, A.18.1.3	14
3.3.9	Limit management of audit functionality to a subset of privileged users.	AU-9(4)	A.12.4.2, A.12.4.3, A.18.1.3	14
Control Family: Configuration Management				
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.	CM-2, CM-6, CM-8, CM-8(1)	A.8.1.1, A.8.1.2	1, 2, 3, 7, 10, 11, 13,

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	CM-2, CM-6, CM-8, CM-8(1)	A.8.1.1, A.8.1.2	1, 2, 3, 7, 10, 11, 13
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	CM-3	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	3, 10
3.4.4	Analyze the security impact of changes prior to implementation.	CM-4	A.14.2.3	
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	3, 10
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	CM-7	A.12.5.1 (ISO control doesn't completely match NIST 800-53)	3
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1), CM-7(2)	A.12.5.1 (ISO control doesn't completely match NIST 800-53)	3
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), CM-7(5)	A.12.5.1 (ISO control doesn't completely match NIST 800-53)	3
3.4.9	Control and monitor user-installed software.	CM-11	A.12.5.1, A.12.6.2	2, 3
Control Family: Identification and Authentication				
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	IA-2, IA-5	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
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-2, IA-5	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.	IA-2(1), IA-2(2), IA-2(3)	A.9.2.1	12, 16
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	IA-2(8), IA-2(9)	A.9.2.1	12, 16
3.5.5	Prevent reuse of identifiers for a defined period.	IA-4	A.9.2.1	12

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
3.5.6	Disable identifiers after a defined period of inactivity.	IA-4	A.9.2.1	12
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
3.5.8	Prohibit password reuse for a specified number of generations.	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
3.5.10	Store and transmit only encrypted representation of passwords.	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
3.5.11	Obscure feedback of authentication information.	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	12, 16
Control Family: Incident Response				
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.	IR-2, IR-4, IR-5, IR-6, IR-7	A.6.1.3, A.7.2.2 (ISO control doesn't completely match NIST 800- 53), A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6	18
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	IR-2, IR-4, IR-5, IR-6, IR-7	A.6.1.3, A.7.2.2 (ISO control doesn't completely match NIST 800- 53), A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6	18
3.6.3	Test the organizational incident-response capability.	IR-3, IR-3(2)	None	18
Control Family: Maintenance				
3.7.1	Perform maintenance on organizational information systems.	MA-2, MA-3, MA-3(1), MA-3(2)	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)	
3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	MA-2, MA-3, MA-3(1), MA-3(2)	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)	
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)	
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)	None	

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control 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	None	
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	None	
Control Family: Media Protection				
3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9	8
3.8.2	Limit access to CUI on information system media to authorized users.	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9	8
3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9	8
3.8.4	Mark media with necessary CUI markings and distribution limitations.	MP-3	A.8.2.2	15
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6	15
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	MP-5(4)	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6	
3.8.7	Control the use of removable media on information system components.	MP-7	A.8.2.3, A.8.3.1	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	A.8.2.3, A.8.3.1	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	A.12.3.1, A.17.1.2, A.18.1.3	8

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
Control Family: Personnel Security				
3.9.1	Screen individuals prior to authorizing access to information systems containing CUI.	PS-3, PS-4, PS-5	A.7.1.1, A.7.3.1, A.8.1.4	
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, PS-4, PS-5	A.7.1.1, A.7.3.1, A.8.1.4	
Control Family: Physical Protection				
3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	PE-2, PE-5, PE-6	A.11.1.2, A.11.1.3	
3.10.2	Protect and monitor the physical facility and support infrastructure for those information systems.	PE-2, PE-5, PE-6	A.11.1.2, A.11.1.3	
3.10.3	Escort visitors and monitor visitor activity.	PE-3	A.11.1.1, A.11.1.2, A.11.1.3	
3.10.4	Maintain audit logs of physical access.	PE-3	A.11.1.1, A.11.1.2, A.11.1.3	
3.10.5	Control and manage physical access devices.	PE-3	A.11.1.1, A.11.1.2, A.11.1.3	
3.10.6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	PE-17	A.6.2.2, A.11.2.6, A.13.2.1	
Control Family: Risk Assessment				
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	A.12.6.1 (ISO control doesn't completely match NIST 800-53)	
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	RA-5, RA-5(5)	A.12.6.1 (ISO control doesn't completely match NIST 800-53)	3
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	RA-5	A.12.6.1 (ISO control doesn't completely match NIST 800-53)	3

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
Control Family: Security Assessment				
3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)	1, 2, 3, 4, 5, 7, 10, 11, 12, 13, 14, 15, 17, 20
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)	1, 2, 3, 4, 5, 7, 10, 11, 12, 13, 14, 15, 17, 20
3.12.3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)	1, 2, 3, 4, 5, 7, 10, 11, 12, 13, 14, 15, 17, 20
Control Family: System and Communications Protection				
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, SA-8	A.8.2.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	13, 19
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	SC-7, SA-8	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3, A.14.2.5	13, 19
3.13.3	Separate user functionality from information system management functionality.	SC-2	None	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	None	
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7, SA-8	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3, A.14.2.5	13, 19
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)	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3	13, 19

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
3.13.7	Prevent remote devices from simultaneously establishing nonremote connections with the information system and communicating via some other connection to resources in external networks.	SC-7(7)	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3	13, 19
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8, SC-8(1)	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	17
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	A.13.1.1	
3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.	SC-12	A.10.1.2	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	
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	A.13.2.1 (ISO control doesn't completely match NIST 800-53)	3
3.13.13	Control and monitor the use of mobile code.	SC-18	None	2
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	None	
3.13.15	Protect the authenticity of communications sessions.	SC-23	None	16
3.13.16	Protect the confidentiality of CUI at rest.	SC-28	A.8.2.3 (ISO control doesn't completely match NIST 800-53)	17
Control Family: System and Information Integrity				
3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53), A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	3, 5
3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53), A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	3, 5

NIST 800-171 Control Number	Control Text	NIST 800-53 Mapping	ISO 27002:2013 Mapping	Relevant 20 Critical Control Mapping
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53), A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	3, 5
3.14.4	Update malicious code protection mechanisms when new releases are available.	SI-3	A.12.2.1	5
3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	SI-3	A.12.2.1	5
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4, SI-4(4)	None	1, 2, 3, 5, 7, 10, 11, 12, 13, 14, 15, 16, 17,
3.14.7	Identify unauthorized use of the information system.	SI-4	None	1, 2, 3, 5, 7, 10, 11, 12, 13, 14, 15, 16, 17