PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL ORGANIZATIONS

USING THE RISK MANAGEMENT FRAMEWORK TO SECURE COVERED CONTRACTOR SYSTEMS

Brian McCoy, CAP

COACT

Table of Contents

Purpose and Intended Audience

Federal requirements for nonfederal organizations to safeguard Controlled Unclassified Information (CUI) are changing. Many of the organizations affected by these changes may underestimate the scope of the requirements and the implications associated with nonconformities. COACT has identified the requirements associated with these specific changes and described how the National Institute for Standards and Technology (NIST) Special

Publication (SP) 800-171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, relates to the changes.

We have utilized our experience with multiple compliance frameworks and risk assessment methodologies to develop a roadmap for achieving and maintaining compliance with emerging regulations. **The purpose of this document is to identify the applicable CUI security requirements and associated federal regulations to assist covered government contractors in recognizing the need to build an effective information security program.**

The requirements described in NIST SP 800-171 apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI and external providers that provide some form of security protection for components that process, store, or transmit CUI. Examples of system components that are in scope for the application of CUI security requirements include: mainframes, workstations, servers, input and output (I/O) devices, network components, operating systems, virtual machines, and applications. The three (3) prerequisites that require the application of the CUI security requirements within nonfederal information systems include:

- When CUI is resident in a nonfederal system and organization;
- When the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
- When there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the publicly-available online CUI Registry maintained by the National Archives and Records Administration (NARA). [1]

Nonfederal organizations that are contracted to process, store, or transmit CUI can limit the scope of CUI security requirements by isolating CUI in separate security domains[2] via secure architectural design strategies in addition to logical separation, physical separation, or a combination of both. This method of structuring applicable information systems to narrow the focus of security control implementation to only pertinent system components can assist nonfederal organizations in reducing costs associated with security and monitoring mechanisms needed to satisfy the appropriate federal regulations, while also ensuring that the security posture of the nonfederal organization is satisfactory to protect organizational mission and business operations.

Controlled Unclassified Information

President Obama signed Executive Order 13556, Controlled Unclassified Information (E.O. 13556) on November 4, 2010, which identifies the need for a government-wide CUI program and establishes NARA as the CUI Executive Agent of the program that is responsible for implementing the order. In addition, E.O. 13556 dictates that CUI categories and subcategories will be used to designate unclassified information that requires the application of safeguarding or dissemination controls to comply with appropriate laws, regulations, and government-wide policies. NARA is the maintainer of the CUI Registry, which is a repository for information, guidance, policy, and requirements regarding the handling of CUI. CUI is defined by NARA as the information that is created or possessed by the government or information that is created or possessed by an organization for or on behalf of the government that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.[3]

There are two (2) types of CUI categories and subcategories, which are categorized as CUI Basic and CUI Specified. CUI Basic includes a subset of CUI that is not covered by specific handling or dissemination controls. General safeguarding requirements are uniformly applied on all CUI Basic categories and subcategories for all agencies. CUI Specific includes a subset of CUI that is covered by specific handling controls that are enumerated by laws, regulations, or government-wide policies. The CUI Specified identifier is used to distinguish information that requires higher or different requirements from the baseline safeguarding requirements that are applied to CUI Basic. Information marked as CUI Specified is identified in the CUI Registry with the applicable handling requirements and associated laws, regulations, and government-wide policies that dictate those requirements. Baseline security requirements, such as those identified in NIST SP 800-171, Rev. 1, apply to CUI Basic whereas the guidance regarding specific controls that must be in place are explicitly defined for CUI Specific categories and subcategories. The CUI Registry contains specific Codes of Federal Regulations (CFRs) applicable for

various categories and subcategories of CUI. The statutory and regulatory language associated with each category or subcategory of CUI can supersede or supplement the minimum CUI requirements identified in 800-171. If the statutory and regulatory language is applicable and existent, it can be found in the CUI Registry using authority links found in individual CUI Category pages. It is important to note that here are higher penalties associated with the failure to adequately protect some of the CUI Specified categories.

CUI Security Requirements

NIST SP 800-171, Rev. 1, prescribes security requirements for federal agencies to safeguard CUI that resides outside of an agency's control. The need for protection and control of CUI when it is processed, stored, or transmitted on nonfederal information systems remains the responsibility of the Federal government. To facilitate the need for security requirements for nonfederal organizations and an updated acquisitions process, NIST led the design of the 800-171 special publication to be used by federal agencies in contract vehicles or other agreements with private industry. Applicable nonfederal organizations are required to meet at least the basic CUI protection level established within 800-171. These requirements for safeguarding CUI ensure that a consistent level of CUI protection is maintained between federal and nonfederal information systems and organizations.

NIST SP 800-171 prescribes both "Basic Security Requirements" obtained from Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and additional "Derived Security Requirements" based on security controls identified in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The requirements from NIST SP 800-53 are not duplicates of federal requirements; rather NIST SP 800-171 is tailored to distinguish between CUI security requirements (i.e. CUI tailoring symbol), requirements that are exclusively federal (i.e. FED tailoring symbol), requirements not directly related to protecting the confidentiality of CUI (i.e. NCO tailoring symbol), and requirements expected to be routinely satisfied by nonfederal organizations without specification (i.e. NFO tailoring symbol).[4] The tailoring guidelines provided in Appendix E within NIST SP 800-171 ensure that applicable security measures meet the level of protection of CUI needed to satisfy, at a minimum, a moderate impact categorization level for confidentiality.

Although containing derived security requirements, NIST SP 800-171 requirements differ significantly from NIST SP 800-53, Rev. 4, which applies to Federal information systems that must comply with the Federal Information Security Modernization Act (FISMA) of 2014; NIST SP 800-171 is intended to be less burdensome. Figure 1 details the number of derived security controls using the Nonfederal Organization (NFO) and CUI tailoring. NIST SP 800-53 contains two-hundred seventy-seven (277) security controls in its moderate baseline, while NIST SP 800-171 results in less than two hundred (200) when combining controls using NFO and CUI tailoring actions.[5]

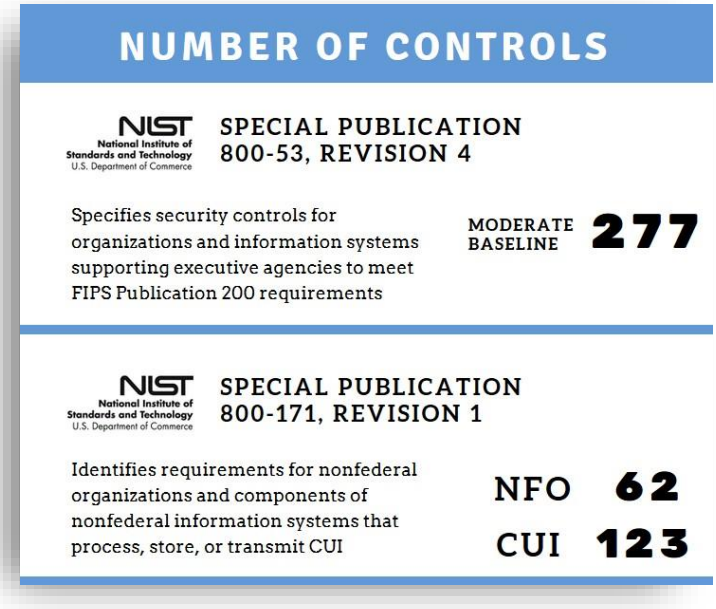

Figure 1. Number of NIST SP 800-53, Rev. 4 Controls

In an effort to promote consistency and comparability, the security safeguards chosen by nonfederal organizations to satisfy the basic and derived security requirements for CUI can be based on existing and recognized security standards and control sets such as NIST SP 800-53, Rev. 4 or ISO/IEC 27001/2. The mapping of controls is utilized by federal agencies to assure that the implementation of security and privacy controls are satisfactory and are reconcilable with their partners. Nonfederal organizations are able to implement security controls directly or use external service providers to satisfy CUI security requirements.

If a nonfederal organization is unable to satisfy a particular security requirement, a compensating security control or alternative implementation can be used, but it must be equally effective to satisfy the CUI security requirement.[6] The guidance provided in NIST SP 800-171 is designed to permit nonfederal organizations to utilize systems, tools, and processes that may already be in place to satisfy the CUI requirements, instead of being required to assume an approach that is specific to executive agencies and other federal organizations.

The requirements are organized into fourteen (14) security requirement families, which are listed in Figure 2. There are fewer families than exist in NIST SP 800-53, Rev. 4. It

should be noted that a subset of basic and derived requirements from the Contingency Planning (CP), Security Planning (PL), and System and Services Acquisition (SA) families have been included in NIST SP 800-171 Media Protection (MP), Security Assessment (CA) and System and Communications Protection (SC) control families for convenience.

Figure 2. Security Requirement Families

Need for Compliance

The Federal Acquisition Regulations (FAR) have been updated in May 2016 to include rule 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*. This updated rule presents a change from the draft rule of 2012, which focused on protecting data, to protecting the information systems, which is in alignment with NIST SP 800-171. However, the rule does not require the full fourteen (14) families of NIST SP 800-171. If a nonfederal organization maintains or operates an information system that processes, stores, or transmits federal contract information, and no superseding contract clause or regulation applies, then only the most basic level of NIST SP 800-171 CUI security requirements are applicable to the covered contractor information system, which includes fifteen (15) security safeguards. It is important to note that the FAR clause does not lessen the responsibility of a nonfederal organization that must meet additional safeguarding requirements specified in other contract or acquisition documentation.

Federal contract information is broadly defined as information that is not intended for public release and is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. Federal contract information does not include information provided by the Government to the public (i.e. publicly accessible websites). The acquisition of Commercial Off the Shelf (COTS) items are excluded from Federal contract information.[7]

The FAR rule requires contracting officers to include FAR 52.204-21 in all solicitations for contracts that may require federal contract information to be processed, stored, or transmitted through a covered contractor information system, which includes those maintained or operated by a subcontractor. Although final, this rule may be considered interim. The Federal Register notes that the FAR rule is one (1) step in a series of regulatory actions that are being developed and implemented to improve the security of information systems and data. The Office of Management and Budget (OMB) issued draft guidance that would mandate covered contractor information systems satisfy all fourteen (14) families of NIST SP 800-171. NARA is finalizing a rule to require contractors to strengthen CUI protection in nonfederal systems and partnered with NIST to develop SP 800-171. The Department of Defense (DoD) revised the Defense Federal Acquisition Regulations (DFARS), a supplement to the FAR that includes acquisition regulations specific to the DoD, mandating contractors with covered contractor information systems or those with covered defense information residing within their information systems meet all fourteen (14) families of security requirements identified in NIST SP 800-171.

The Federal Acquisition Regulatory Council is working to amend the FAR to include contract language in acquisitions that will apply to nonfederal organizations. The Chief Information Officer (CIO), Chief Administrative Officer (CAO), Chief Information Security Officer (CISO), privacy officer, and other stakeholders within each Federal agency are responsible for applying the guidance. The OMB Guidance, which was issued in 2015, addresses the need to include contract clauses in federal acquisitions that would mandate contractors to implement security

safeguards and processes to demonstrate compliance with CUI security requirements. The guidance recommends the inclusion of contract language that addresses:

- Implementation of security controls;
- Cyber incident reporting;
- Security assessments of contractor internal systems;
- Information security continuous monitoring; and
- Increased business due diligence.

The clause in DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, requires that affected nonfederal organizations implement the CUI security requirements no later than December 31, 2017. This requirement also applies to subcontractors of those organizations. There is an additional regulation imposed on DoD contractors to notify the DoD CIO within thirty (30) days of the award of the contract regarding any NIST SP 800-171 security requirements that are not implemented at the time of award. In addition, the DoD contractor must provide an explanation if a requirement is not applicable or if a compensating security safeguards or alternative implementation will be in place to satisfy a particular CUI security requirement. Similar to other security risks or vulnerabilities, failure to meet the minimum CUI requirements identified in NIST SP 800-171 can result in:

- Damage to the standing or reputation of the affected nonfederal organization;
- Financial loss or liability associated with the affected nonfederal organization;
- Harm to government programs or public interests; and
- Unauthorized release of sensitive information.

There is also an unexpected possibility of a breach of contract with the federal government if a nonfederal organization is found to be noncompliant. In addressing this possibility, FAR 52.204-21 states that as long as safeguards are in place, then failure of the security controls or mechanisms to adequately protect the CUI will not constitute a breach of contract. In addition to the legal and regulatory requirements that mandate the implementation of security measures to protect CUI, the realization of consistent security standards at a moderate level assists in preventing adverse impacts to the missions and business operations of the Federal Government.

Basic Security Safeguards

The most basic level of CUI security requirements involves the implementation of fifteen (15) security safeguards that are established in FAR 52.204-21.[8] The security safeguards identified in the FAR clause can be categorized based on the security requirement family to which each safeguard applies. It is important to note that FAR 52.204-21 does not mean that the government contractor can forego implementing security controls to meet other safeguarding requirements identified by agencies or the requirements established by E.O. 13556.

Access Control

Contractors are required to limit information system access to authorized users, processes acting on behalf of authorized users, and devices. The requirement to limit information system access also applies to other information systems. Connections to and use of external information systems by the covered contractor information system must also be verified and controlled. External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. These information systems may be used to process, store, or transmit CUI from a covered contractor information system.

Contractors are required to limit information system access to the types of transactions and functions that authorized users are permitted to execute. The access control system must limit access based on the concept of separation of duties and the principle of least privilege. In addition, information posted or processed on covered contract information systems with a publicly accessible component must be controlled via review and authorization processes. The general public is not authorized to access nonpublic information (i.e. information classified as CUI).

Identification and Authentication

Covered contractor information systems are required to identify information system users, processes acting on behalf of users, and devices. In addition, the information system must authenticate the identities of those users, processes, and devices before permitting access. The identification and authentication best practices that contractors should implement include: using replay-resistant authentication mechanisms, authenticating to a cryptographic module, multifactor authentication, and managing identifiers and authenticators appropriately. Identifier management involves selecting and assigning unique identifiers for users, groups, roles, and devices following receipt of authorization by the appropriate personnel. Authenticator management involves the definition and implementation of lifetime restrictions, reuse conditions, and authenticator strength requirements (e.g., password complexity, length). Authenticators must be protected from unauthorized disclosure and modification.

Media Protection

Contractors must also ensure that information system media that contains federal contract information is sanitized or destroyed before disposal or release for reuse. Both digital and non-digital media are considered in scope for sanitization or destruction. Examples of digital media include magnetic tapes, external/removable hard drives, flash/thumb drives, and compact disks, while non-digital media includes hard copy materials (e.g., paper printouts). The contractor must coordinate with the appropriate government entity to verify that the sanitization mechanisms that are used meet the media protection requirements identified in acquisition documentation in addition to applicable laws, regulations, and government-wide policies. Examples of media sanitization techniques include: clearing (e.g., overwriting), purging, and physical destruction (e.g., pulverize, shred).

Physical Protection

FAR 52.204-21 stipulates that physical protection safeguards must also be in place to limit physical access to covered contractor information systems, equipment, and the respective operating environments to authorized individuals. Controls that can be used to limit physical access include the use of physical access devices (e.g., cipher locks, card readers) in addition to badges and smart cards. Contractors must enforce physical access authorizations at entry and exit points to the facility in addition to areas where covered contractor information systems are located. In addition, the contractor must maintain access audit logs and manage physical access devices including the inventorying of such devices periodically. Any visitor to the facility where a covered contractor information system resides must be escorted at all times by organizational personnel and visitor activity must be monitored via visitor access logs and surveillance cameras.

System and Communications Protection

If a covered contractor information system has any publicly accessible components, the contractor is required to implement subnetworks to ensure physical or logical separation from internal networks. There must also be mechanisms in place to monitor, control, and protect communications at external information system boundary and key internal boundaries. Boundary protection devices such as proxies, gateways, routers, firewalls, and encrypted tunnels must be deployed at strategic locations and configured appropriately to effectively manage system interfaces. In addition, the boundary protection device(s) must be capable of monitoring the information (e.g., CUI) that is transmitted or received by the covered contractor information system.

System and Information Integrity

FAR 52.204-21 also requires contractors to utilize malicious code protection mechanisms and establish a flaw remediation capability. Malicious code protection mechanisms, which include various technologies and methods, must be employed at information system entry and exit points in addition to strategic and ad hoc locations within the system. Examples of entry and exit points include: firewalls, mail servers, web servers, workstations, and mobile devices. The contractor personnel that are assigned to manage the malicious code protection mechanisms must ensure that the mechanisms are updated when new releases are available and prior to scans of the covered contractor information system. The malicious code protection mechanisms must also be configured to perform real-time scans of files that originate from external sources when those files are downloaded, opened, or executed. Any flaws that are identified within the covered contractor information system must be reported, tracked, and remediated in a timely manner. The flaw remediation processes should be coordinated with a change control process to ensure changes associated with flaw remediation activities are tested and approved before implementation within a production environment.

Risk Management Framework (RMF)

Nonfederal organizations that currently contract with the Federal Government to provide information technology services that must meet the CUI requirements and nonfederal organizations that hope to do business with the Federal Government in the future can utilize the security requirement information defined in NIST SP 800-171 to develop an effective information security program. Since the CUI requirements were developed using security requirements from FIPS PUB 200 and derived security requirements from the NIST SP 800-53, Rev. 4 moderate security control baseline, nonfederal organizations can use the NFO and CUI tailored controls identified in Appendix E within NIST SP 800-171 to implement the security controls that should be routinely satisfied without specification by the federal government and those directly related to protecting the confidentiality of CUI. The implementation of the security controls contributes to an effective risk-based information security program with the necessary policies, procedures, and practices needed to support such a program.

The requirements described in NIST SP 800-171 apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI and external providers that provide some form of security protection for components that process, store, or transmit CUI. Nonfederal organizations that are contracted to

process, store, or transmit CUI can limit the scope of CUI security requirements by isolating CUI in separate security domains via secure architectural design strategies in addition to logical separation, physical separation, or a combination of both. This method of structuring applicable information systems to narrow the focus of security control implementation to only pertinent system components can assist nonfederal organizations in reducing costs associated with security and monitoring mechanisms needed to satisfy FAR 52.204-21 and DFARS 252.204-7012, while also ensuring that the security posture of the nonfederal organization is satisfactory to protect organizational mission and business operations.

The RMF, which is defined and explained in NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, can be used to demonstrate compliance with FAR 52.204-21 and DFARS 252.204-7012. The six (6) steps of the framework, which are identified in Figure 3, ensure that a nonfederal organization's information security program can incorporate applicable information systems that require CUI protections into a process where security safeguards used to protect organizational systems are documented, authorized, assessed, and monitored. If a nonfederal organization has not developed or implemented a mature information security program, then organizations that must comply with the requirements of the FAR and DFARS can leverage the recent compliance requirements as an opportunity to improve multiple areas of organizational security programs using the available guidance and security best practices. Commitment to an information security program assists in protecting organizational assets, including those that process, store, or transmit CUI by formalizing the processes needed to secure information and information systems including: establishing information security roles and responsibilities; documenting policies and procedures in accordance with established legal and regulatory requirements; and taking a risk-based approach to decision-making that could impact the security state of information and information systems.

A mature information security program supports security assessment and authorization activities that are used throughout the RMF to verify the implementation of security safeguards. In addition, an information security program assists in maintaining the security of information and information systems throughout the system development life cycle (SDLC) and during routine operations. Following the development and documentation of policies and processes to address security requirements identified in applicable laws, regulations, and contractual language, nonfederal organizations are responsible for demonstrating compliance and maintaining the security of CUI and appropriate information systems. The information security and system documentation can be used as a reference point throughout the RMF to validate that security controls and mechanisms are in place and operating as intended. The areas of the information security program associated with the CUI security requirements can be tested and validated using the RMF to demonstrate compliance.

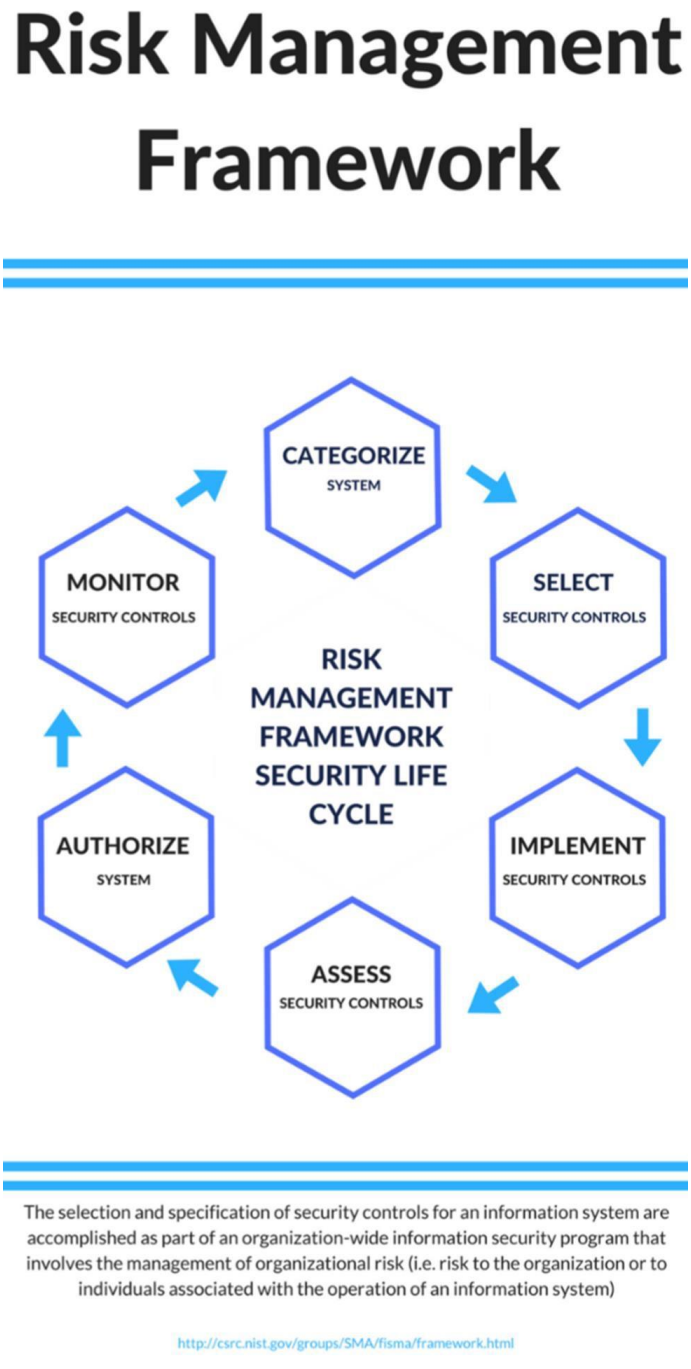

Figure 3. NIST Risk Management Framework

The traceability of NIST SP 800-53, Rev. 4 security controls to the CUI security requirements identified in NIST SP 800-171 allows for the documentation of information related to system components where CUI resides in standard documents such as a System Security Plan (SSP). Using the six (6) steps of the RMF, a nonfederal organization can

determine the information types associated with the CUI, implement security safeguards to protect the CUI, and document the safeguards. In addition, the nonfederal organization can utilize the tailoring criteria in Appendix E of NIST SP 800-171 to implement security controls that are expected to be routinely satisfied by nonfederal organizations without specification and those directly related to protecting the confidentiality of CUI. Information obtained from security assessment and authorization activities can be submitted to contracting officers to demonstrate compliance in an effort to remain in good standing with Federal agencies, maintain contractual obligations, and avoid liabilities associated with noncompliance. The five (5) steps that nonfederal organizations should take to ensure compliance with FAR 52.204-21 and DFARS 252.204-7012 include: performing a gap analysis and readiness assessment; documenting the information security program; contracting an independent third party to perform an assessment of the information system; remediate findings identified during the assessment; and continuously monitor the information system.

Readiness Assessment

Before developing security documentation for a covered contractor information system, nonfederal organizations should participate in a readiness assessment. The readiness assessment is used to identify the prerequisites for compliance and establish the boundaries of the system where CUI is stored, processed, and/or transmitted. The readiness assessment is also executed to determine the current security safeguards that are in place and quantify the scope of the effort to become compliant and maintain compliance with the applicable acquisition regulation. The scope of the safeguarding requirements in the CUI regulations is limited to the confidentiality security objective and does not include requirements that have been identified as uniquely federal. In addition, the potential impact on the organization, assets, or individuals following a loss of confidentiality must be at a Moderate level or higher for the CUI requirements to apply. It is recommended that nonfederal organizations implement security controls to meet the CUI security requirements and the requirements expected to be routinely satisfied by nonfederal organizations using the tailoring guidance documented in NIST SP 800-171.

Security Documentation

Following the readiness assessment, the nonfederal organization must document the security requirements for the covered contractor information system and describe the security controls that are in place or planned for meeting those requirements. This information must be documented in a System Security Plan (SSP) in order to comply with CUI Basic Security Requirement 3.12.4. In addition to the SSP, the nonfederal organization should develop the appropriate information system policies and procedures to address the operation of the information system and the implementation of the information security program. During the documentation development effort, the nonfederal organization should identify any gaps in the implementation of security controls and remediate the potential vulnerabilities via deployment or enhancement of security safeguards within the authorization boundary of the information system.

Independent Assessment

The nonfederal organization seeking to demonstrate compliance with FAR 52.204-21 and DFARS 252.204-7012 should utilize an independent third-party assessment organization to assess the covered contractor information system. During the fourth step of the RMF, the information system is assessed to determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting applicable CUI security requirements. To ensure impartiality and independence from the nonfederal organization, the assessor selected must not represent a mutual or conflicting interest with the organization, act as management or personnel employed at the organization, or place themselves in positions of advocacy for the organization. The assessor(s) will perform hands-on testing, interview technical and management personnel, and review documentation, which are the three (3) assessment methods used to evaluate security controls to determine effectiveness (i.e. Examine, Interview, and Test). Artifacts will be obtained during the assessment and used as evidence to verify the security state of the information system and identify any deficiencies. The documentation generated following an assessment includes a Security Assessment Report (SAR), Risk Assessment Report (RAR), and Plan of Action and Milestones (POA&M). Using the results of the assessment, the nonfederal organization must implement corrective actions to remediate any identified deficiencies. The remediation of findings may include the creation of missing documentation, deployment of security tools, or improvement of existing processes to comply with the appropriate security requirements identified in NIST SP 800-171, acquisition documentation, and/or the CUI Registry. The assessment results and remediation efforts will be reviewed by the designated approving authority and if the risk associated with the operation of the information system is acceptable, an Authority to Operate (ATO) letter or equivalent certifying document will be created and signed.

Continuous Monitoring

Following the initial security assessment and issuance of an ATO, the nonfederal organization should engage in continuous monitoring in an effort to maintain awareness of

the security state of the information system. The final step of the RMF process involves the continuous monitoring of security controls to include periodically assessing control effectiveness, performing configuration management processes, engaging in incident response activities, and regularly reporting the security state of the system to the appropriate personnel. An Information Security Continuous Monitoring (ISCM) strategy should be developed and implemented using guidelines described in NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. A continuous monitoring program will support the establishment of metrics and the improvement of existing metrics that can be used to report the security status of the information system to organizational officials. Metrics are expected to mature during the execution of continuous monitoring processes as information obtained from lessons learned and remediation activities is incorporated to provide further insight into the security posture of the information system and information security program overall. The identification of metrics and a schedule for ongoing assessments and reporting of security information to organizational officials should be developed to ensure that documentation is reviewed and updated periodically, and a subset of applicable security controls are assessed to demonstrate continued compliance.

Conclusion

Contractors that would like to work with the government must continue to maintain awareness of emerging security requirements and the impact of new regulations on their information systems and information security programs. Organizations that wish to continue doing business with the government must review contracts and acquisition regulations with added scrutiny to ensure compliance and provide adequate security to their government clients.

Although there are several ways to demonstrate and maintain compliance with the new CUI regulations, COACT has determined that utilizing the RMF provides a consistent and comprehensive approach to addressing the security requirements. The RMF can be used to improve the security of the information system and will support scoping of the CUI to establish an appropriate authorization boundary and reduce the burden of these new security concerns on nonfederal organizations.

COACT

COACT, Inc. is a leading service-disabled veteran owned small business and test laboratory that provides Global IT Security Services, Accredited Evaluations and Testing, and Evidence-Based Compliance Services for traditional, hybrid, and cloud-based systems serving governments and private industry. COACT is a leader in risk management and compliance. COACT is ISO 9001:2015 compliant and a Federal Risk and Authorization Management Program (FedRAMP) Accredited Third Party Assessment Organization (3PAO). COACT tiered service offerings range from focused efforts to address specific security objectives, to providing full information security programs for clients in commercial, healthcare, regulatory, defense, and intelligence domains.

Notes

[1] See Ross et al for additional information regarding the applicability of CUI requirements. NIST SP 800-171, Rev. 1 identifies the circumstances when the CUI security requirements are applicable to a nonfederal organization and how to determine if a contractor information system must comply with FISMA requirements or CUI security requirements (2-3).

[2] See Ross et al for strategies that can be utilized by contractors to limit the scope of CUI security requirements and alleviate the resources needed to secure CUI per contractual obligations and acquisition regulations. The strategies describe the approaches to securing CUI in the context of cost reductions and overall efficiency (4).

[3] See NARA for definitions and additional information regarding the key elements of CUI, categories and subcategories of CUI, and regulatory information associated with CUI. NARA is the CUI Executive Agent responsible for maintaining the CUI Registry, which contains the various categories and subcategories associated with CUI.

[4] See Appendix E in Ross et al for tailoring guidance information and the identification of NIST SP 800-53, Rev. 4 security controls that can be used to satisfy CUI basic and derived security requirements. Both NFO and CUI tailored controls are discussed in this paper to quantify the level of effort required to establish an adequate information security program and address the assumption that most nonfederal organizations will implement at least a subset of the NFO tailored controls.

[5] See Joint Task Force Transformation Initiative for additional information regarding the security controls that are in scope for the Moderate security control baseline. The NFO and CUI tailored controls are mapped to the security controls documented in NIST SP 800-53, Rev. 4 for uniformity and convenience when determining compliance with CUI security requirements.

[6] See DFARS 252.204-7012 for additional information regarding the safeguarding, disclosure, and reporting requirements for covered contractor information systems. The regulation contains guidance regarding how to comply with the new CUI requirements and maintain compliance during contract lifetimes.

[7] See FAR 52.204-21 regarding the exclusion of COTS products from the final CUI safeguarding rule. It is important to note that COTS products that are acquired and used to store, process, or transmit CUI are the responsibility of the purchasing Agency to authorize within the boundaries of an appropriate information system.

[8] See FAR 52.204-21 for regulatory information regarding the implementation of the fifteen (15) security safeguards that are required, at a minimum, for covered contractor systems. Note that the fifteen (15) safeguards do not relieve the contractor from adhering to other CUI security requirements defined in acquisition documentation, regulations, or the CUI Registry.

Works Cited

Computer Security Division. (2006). *Minimum Security Requirements for Federal Information and Information Systems* . (Federal Information Processing Standards Publication 200) . Retrieved from https://www.nist.gov/publications

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., … Stine, K. (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* (NIST Special Publication 800-137). Retrieved from https://www.nist.gov/publications

Federal Acquisition Regulation, 48 C.F.R. § 252.204-7012 (2016).

Federal Acquisition Regulation, 48 C.F.R. § 52.204-21 (2016).

Joint Task Force Transformation Initiative. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. (NIST Special Publication 800-53, Rev. 4) . Retrieved from https://www.nist.gov/publications

National Archives and Records Administration (2017, January 25). CUI Glossary. Retrieved from https://www.archives.gov/cui/registry/cui-glossary.htm

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* (NIST Special Publication 800-171, Rev. 1) . Retrieved from https://www.nist.gov/publications

Glossary of Terms

Authorization	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
Authenticator	The means used to confirm the identity of a user, process, or device (e.g., user password or token).
Availability	The property of being accessible and useable upon demand by an authorized entity.
Confidentiality	The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
Controlled Unclassified Information	Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.
Covered Contractor Information System	Unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
CUI Basic	Subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic per the uniform set of controls set forth in NIST SP 800-171 and the CUI Registry.
CUI Executive Agent	Executive agency responsible for implementing the executive branch-wide CUI Program and overseeing federal agency actions to comply with Executive Order 13556.
CUI Registry	Online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
CUI Specific	Subset of CUI for which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use regarding the handling or dissemination of CUI.
Environment of Operation	The physical, technical, and organizational setting in which an information system operates, including but not limited to: missions/business functions; mission/business processes; threat space; vulnerabilities; enterprise and information security architectures; personnel; facilities; supply chain relationships; information technologies; organizational governance and culture; acquisition and procurement processes; organizational policies and procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs.
External Provider	A provider of a system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
Federal Information Security Management Act of 2002	A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB.
Federal Information Security Modernization Act of 2014	Amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.
Flaw Remediation	The process of identifying, reporting, tracking, and correcting information system flaws.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Continuous monitoring involves the collection of information in accordance with pre-established metrics and the utilization of information readily available in part through implemented security controls.

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Impact Level	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Least Privilege	Principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Malicious Code	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Nonfederal Organization	An entity that owns, operates, or maintains a nonfederal system.
Organizational User	An organizational employee or an individual the organization deems to have equivalent status of an employee (e.g., contractor, guest researcher, individual detailed from another organization).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Scoping Guidance	Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.
Readiness Assessment	An assessment that is performed to identify existing security capabilities that are used to determine the current level of compliance with a standard or regulation.
Remediation	The act of correcting a vulnerability or eliminating a threat.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Management Framework	A structured approach that is used to oversee and manage risk for an enterprise. The Risk Management Framework involves the building of information security capabilities into information systems through the application of state-of-the-practice management, operational, and technical security controls; maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, and other organizations arising from the operation and use of information systems.

Sanitization	Process to remove information from media such that information recovery is not possible.
Separation of Duties	Concept that no single user should be assigned the level of privileges to misuse an information system. The purpose of separating duties is to minimize the risk and occurrence of collusion among individuals by assigning individuals of varying skills or interests to separated tasks.
System Development Life Cycle	Scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
Tailored Controls	The resulting security control baseline that is modified based on: (i) application of scoping guidance; (ii) specification of compensating security controls; and (iii) specification of organization-defined parameters in the security controls.