SOLUTION BRIEF

Tripwire Solutions and NIST 800-171

Impacts on Business Between DoD/Civilian Agencies and Contractors

The NIST SP 800-171 *"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"*[1] describes security requirements for Non-Federal entities (including some quasi-official agencies) to meet federal mandates for marking, safeguarding, transporting, disseminating, reusing, and disposing of Federal CUI – Controlled Unclassified Information[2].

Federal security managers expect that most federally run systems are actively engaging with FISMA compliance for protecting federal data and systems. However, as we all know, federal information does not remain only in federally operated systems. Data and IT systems connect via the internet and other networks for business, operations and research. Information about citizens, banking and finance, research and development, and many other federal connected systems transmit data outside the federal networks—and their security compliance standards. So it makes sense that FISMA would adapt to address more than the original scope of perceived threats and specifically address systems and data security that inter-agency networks, vendors, contracts and supply chain puts at risk.

In plain English, any company or organizations that contracts with the federal government and handles, processes or stores sensitive types of government information must comply with the security controls described in SP 800-171. This instruction impacts a range of "external service providers," including state and local governments, non-profits, materials vendors and systems integrators. The effective date was 2017.

"Controlled Unclassified Information" (CUI) is a categorization of information that encompasses any information that could be considered non-public/sensitive[3]. This information used to be known as "Sensitive but Unclassified" (SBU). SBU changed to CUI as part of government-wide efforts to better mark, manage and address risks to this information.

Examples of CUI

Financial: Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.

Research: Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. Includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.

Agriculture: Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.

Legal: Information related to proceedings in judicial or quasi-judicial settings.

There are subcategorizations of CUI that contractors must understand to implement the NIST instructions, but assume, for the most part, that many contractor organizations will have to comply. For deeper understanding of CUI handling rules, look to the National Archive and Records Administration (NARA). NARA manages a CUI Registry site (archives.gov/cui), which provides a central location to find all laws, regulation and other information about CUI. NARA documentation[4] on CUI is being adjusted to reflect NIST 800-171, and NARA released new instructions for the Federal Acquisition Regulation (FAR) in 2017 that specifically addressed all contracts that may use/share CUI data.

The DoD has been more aggressive with their Interim Rule on acquisitions which amended DFARS 252.204-7012. This new clause gave contractors until December 2017 to fully implement NIST SP 800-171.

FISMA Background

In 2002, the U.S. Congress passed the Federal Information Security Management Act, or FISMA, as result of concern that technology and computing practices were inconsistent and insecure—leading to enormous risk to federal data and systems. The law assigned the National Institute of Standards and Technology (NIST) to create the operational guidance that would be used to apply security, measure and manage risk to data and systems. It was a very different world in 2002, and while many chaffed at the cost and complexity of applying consistent security controls, most organizations have come to recognize the value of normalized process and improvement of cyber security.

The NIST document SP 800-171 includes the methods by which a federal agency and the external service providermust determine the level of CUI information in scope to evaluate and ensure security controls. The guide also provides specific security requirements to be applied to computer systems and networks associated with the information processed—and the risks inherent to—the contractor's environment.

Which Controls are Important for CUI?

There are 110 control requirements in NIST SP 800-171 organized in "families" of controls similar to other NIST-authored guidance. The control requirements are indicated as either "basic" or "derived." The contractor should use NIST guidance FIPS Publication 200 and NIST SP 800-53 rev 4 to examine more details about the controls.

Control Family	Basic Controls	Derived Controls
3.1 Access Control	2	20
3.2 Awareness and Training	2	1
3.3 Audit and Accountability	2	6
3.4 Configuration Management	2	7
3.5 Identification and Authentication	2	9
3.6 Incident Response	2	1
3.7 Maintenance	2	4
3.9 Personnel Security	2	0
3.10 Physical Protection	2	4
3.11 Risk Assessment	4	0
3.13 System and Communications Protection	2	14
3.14 System and Information Integrity	3	4

For most organizations, the process of identifying the CUI data managed, and which systems and networks will be in scope can be time consuming and revealing. Reorganization of network or system design may be warranted to logically isolate CUI systems and lessen the impact of security controls on all other networks and systems.

Once the location and boundaries are defined, this will be the first step in achieving compliance and starts the documentation of the compliant systems in accordance with supplemental guidance (i.e. NIST guidance such as 800-37, FIPS 199, FIPS 200, 800-60, 800-53, 800-137, and 800-30—see references).

The significant goal is to apply controls as described in the control families. Many of these control requirements can be met with Tripwire tools along with documentation of processes and procedures.

We also recommend you review Tripwire's Detailed Mapping of NIST 800-171 (available on request). It provides the affected organization with the information from NIST 800-171 describing each requirement and how Tripwire can help you achieve compliance for your specific network or system security requirements.

What Does This Have to do with FISMA?

While NIST 800-171 addresses federal and defense contractors, these new instructions do not address service providers who already process CUI or other information on behalf of federal government entities (e.g. contracts to run federal systems). Systems and information processing done for the federal government must already meet FISMA requirements, which are more specific and severe than the SP 800-171.

The NIST 800-171 is part of guidance associated and aligned with FISMA rules. FISMA stipulates a process to assess, document, approve and apply security controls to federal systems. FISMA guidance includes commonly referenced guides and instructions such as NIST SP 800-36, SP 800-53, NIST SP 800-60, FIPS-199 and FIPS-200. Those core FISMA guides are also referenced by the SP 800-171, and are expected to be used in conjunction with the protection of CUI by external non-federal entities.

NIST 800-171 Control Family, Basic Security Requirements	Tripwire Coverage
3.1 Access Control	
3.2 Awareness and Training	
3.3 Audit and Accountability	
3.4 Configuration Management	
3.5 Identification and Authentication	
3.6 Incident Response	
3.7 Maintenance	
3.8 Media Protection	
3.9 Personnel Security	
3.10 Physical Protection	
3.11 Risk Assessment	
3.12 Security Assessment	
3.13 System and Communications Protection	
3.14 System and Information Integrity	

How Does This Impact Acquisition?

The NIST 800-171 is one of a number of changes impacting federal acquisitions. Starting with the DoD's focus on "security supply chain (SSC) management" several years ago, there has been a steady pace of regulatory and other changes to the rules governing acquisitions.

The provisions in FAR 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems" and DFARS 252.2014-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"[5] (which designates NIST SP 800-171 as the security framework to meet DFARS compliance) are the two most important regulations for both federal buyers and contractors to pay attention to.

The impact to most federal organizations and contractors is that new guidance, such as NIST 800-171, drives organizations to build additional security rules into contracts and makes compliance to these rules part of the selection process. This could impact both existing contracts and future contracts.

Agency and other federal entities should not assume that procurement processes will be able to advise the buyer organization or the vendor in a timely manner. The deadline for the NIST 800-171 to go into effect was December 2017. It is incumbent on the vendor community to pay close attention to these rules and updated guidance to ensure they are able to meet federal rules, and remain "in sync" with their customers' procurement teams.

Key Takeaways

The NIST 800-171 is not complete enough (at present) to support a compliance program. A compliance program will have audit/assessment guidance and further instructions on implementation and interpretation.

There will be two key items to pay attention to:

» NARA (the government organization responsible for managing the CUI rules) must publish a new FAR ruleset to institute and clarify the use of NIST 800-171 for the protection of CUI by suppliers and non-federal entities. Until the single FAR clause takes place, agencies and federal buyers should still reference NIST 800-171 as requirements, but this will vary by organization as to consistency of implementation and interpretation.

» NIST must publish companion guidance (as with other guides like 800-53) to provide assessment and auditor support for the implementation of security controls to meet the 800-171 requirements. When published, the companion guide will be marked 800-171A.

Conclusion

FISMA security compliance is an evolving program that is using the NIST SP 800-171 to address (in part) the broader topics of data security and supply chain security. This is an acknowledgement that the federal ecosystem of vendors, partners and suppliers represents the reality of how interconnected the modern economy is. There are a significant number of stakeholders in the supply chain for the federal government, which means that sensitive data must be protected throughout its entire lifecycle. This focus is driven by recognition that protection measures must include government contractors and other non-federal entities.

For Non-Federal organizations that will be impacted by NIST SP 800-171, this is the time to do some homework. While the companion guide is still unpublished, that does not mean that an organization should stand by. It would be a solid recommendation to have organizations start with the existing FISMA guidance (such as NIST SP 800-53A) to examine the likely means to best secure IT/Network systems and CUI data. There is a lot of information, supplemental information and tools that already exist to address many of the NIST common technical controls.

It is interesting that the DFARS amendment is already in play for DoD vendors with a December 2017 deadline, prior to a similar directive for civilian vendors. However, if you are a civilian side vendor, you may want to get ready to act since NIST and the Department of Commerce are expected to release updates very soon—and may try to sync with the DoD deadline.

1 NIST Special Publication 800-171, Rev 1 was published in Dec 2016

2 See Executive Order 13556 – Controlled Unclassified Information (CUI)

3 Taken from https://www.archives.gov/cui/registry#categories

4 NARA CUI Marking Guide, Dec 2016 [for federal agencies, but likely to impact contractors] https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf National Archives and Records Administration, Controlled Unclassified Information Registry. [NARA CUI concept dictionary] https://www.archives.gov/cui/registry/category-list

5 Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS)