It’s Just Results Compliance Services

DFARS 252.204-7012 & NIST 800-171 A Requirement for Policies

Sustainable Security Through Rapid Compliance

A Requirement for Policies

Improved Security

The Department of Defense (DoD) has long sought improved security throughout the DoD's supply chain. Improved security through compliance is the selected path for hardening and safeguarding information systems from cyber incidents. The compliance requirements are defined in the DoD's Defense Federal Acquisition Regulations (DFARs) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. The initial final rule was published in 2013 and DoD has been working with industry ever since to achieve implementation throughout the supply chain.

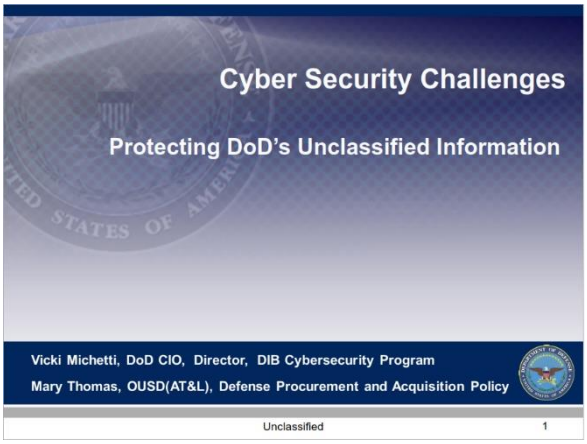

Figure 1- Defense Industry Day Presentation

Government Contractor Requirements

The Department of Defense's Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, issued a memorandum establishing a deadline for contractors to have a System Security Plan (SSP) and a Plan of Action and Milestones (POA&M) in place by December 31, 2017. This was to accelerate the fulfillment of the requirements defined in the DoD's acquisition regulation 252.204-7012 for implementing security controls for Controlled Unclassified Information (CUI).

This regulation placed many requirements on suppliers and their vendors for meeting standards established by DoD and used the Department of Commerce's (DOC's) National Institute and Standards *(NIST) Special Publication SP 800-171 Rev1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* as its foundation. The NIST framework has 110 security controls and additional expectations contained in Appendix E for Non-Federal Organizations (NFOs). Government contractors servicing the Department of Defense are expected to follow/implement these controls.

The Significant Role of Policies

The DFARS requirement, including NIST 800-171, specifies a variety of control types including hardware, software, configuration, and policy/process. In our scan of the supply chain we are seeing many contractors initially focus in on some of the technical controls to safeguard information that requires being protected. They are making progress on a variety of initiatives such as access control, system monitoring, and incident response. They are not making as much progress with policies.

There are several implementation challenges for smaller organizations. One significant gap we regularly come across is in the development and implementation of policies. Small organizations typically do not have mature policies. They struggle with policy development. In some cases, there are no policies, in other cases, they are too generic and yet in others contain so much language it is hard for business

A Requirement for Policies

enterprise managers to understand the policies, let alone communicate their expectations to staff and contractors.

In conducting audits against the DFARS and NIST requirements we look for evidence of mature policy environments. We define mature environments as ones where the business enterprise has written policies with well-defined activities and accountability assigned to individuals. We also look for evidence of procedures, standards, metrics, and governance (review of policies and management of policy activities).

Policy implementation is an expected safeguarding measure (Page 41 of the June 2017 DOD Industry Information Day) is shown in Figure 2 shown here.

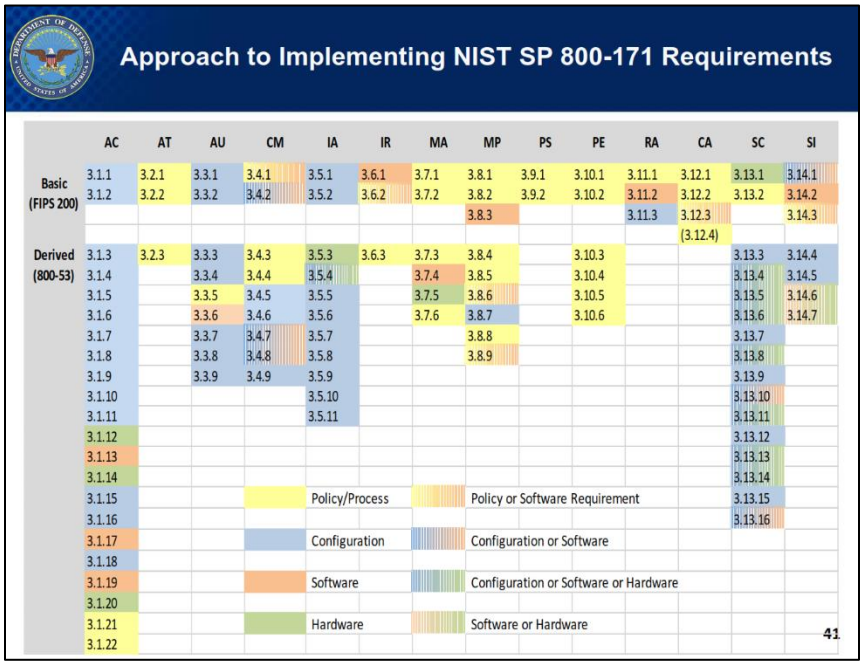

Figure 2-2017 DoD Industry Day Control Chart

Policies are the bridge between risk assessment and development of objectives with the actual day to day management of your technology and security infrastructure. Policies are the mechanism to document decisions made by a business enterprise. Auditors use these policies to understand the security decisions and controls selected by the business enterprise and then audit the actual environment against the stated policies and controls.

Security policies have a key role in nearly 40 of the 110 controls in the special publication. NIST is explicit on the requirement and value of policies in 800-171. In addition, Appendix E has additional policy requirements not depicted in Figure 1 above, as they are considered foundational and expected for all information security programs.

NIST SP 800-171, draws from, is a streamlined version of NIST SP 800-53. NIST SP 800-171 was designed specifically for Non-Federal Organizations (NFOs). Their non-federal information systems. NIST 800-171 is mandatory for defense contractors who have the DFARS 252.204-7012 clause in any contract. Even though 800-171 is a streamlined version of 800-53, many of the concepts and requirements directly flow down from 800-53.

A Requirement for Policies

One particular phrase, is critical and extremely important. That is the definition of the term "IT security policy". NIST defines IT security policy as the "documentation of IT security decision."

Statement	Document	Page
IT security policy is defined as the "documentation of IT security decisions."	NIST.SP.800-53	Page 45

Table 1- IT Security Policy Definition

The documentation of IT decisions shows a certain level of maturity in an information security program. A more ad-hoc information security program would have some technologies deployed (e.g. firewalls, threating monitoring), but not necessarily defined by policy. When policy is not defined, there is no construct to the security architecture, and leads to a much higher degree of potential exploitability of the infrastructure. An audit finding showing great deficiencies in policies reveals a longer path towards conformance to the regulations.

NIST SP 800-171

Policy implementation is an **expected safeguarding measure** of NIST SP 800-171 and is specified in Section 2.2, Development of Security Requirements (see Footnote 16 on Page 6) and shown in the *Table 2* below.

Statement	Document	Page
The security requirements developed from the tailored FIPS Publication 200 security requirements and the NIST Special Publication SP 800-53 moderate security control baseline represent a subset of the safeguarding measures that are necessary for a comprehensive information security program. The strength and quality of such programs in nonfederal organizations depend on the degree to which the organizations implement the security requirements and controls that are expected to be routinely satisfied without specification by the federal government. **This includes implementing security policies, procedures, and practices that support an effective risk-based information security program.** Nonfederal organizations are encouraged to refer to Appendix E and Special Publication 800-53 for a complete listing of security controls in the moderate baseline deemed out of scope for the security requirements in Chapter Three.	NIST.SP.800-171r1	Page 6

Table 2- Expected Safeguarding Measure

Policies are considered required safeguarding measures in any security program. NIST 800-171 has fourteen security families and defines the security requirements related to each family. Policies are needed for all 14 families and many families will have more than one policy. For example, in our client

A Requirement for Policies

engagements, we have developed a policy governance model that has over 40 policies that are aligned to meet the specific requirements of the NIST SP 800-171.

In addition, the appendix also lists expectations for Non-Federal Organizations (NFOs) that is derived from NIST SP 800-53. In the appendix, as shown in *Table 3* below, the publication says that the implementation of policies is expected to be routinely satisfied by Non-Federal Organizations without specification (Page 51 of NIST SP 800-171). Without specification means that it is not being prescribed as part of the 110 controls in NIST SP 800-171, but rather, it is expected in any security program.

Statement	Document	Page
NFO **Expected to be routinely satisfied** by nonfederal organizations without specification	NIST.SP.800-171r1	Page 51

Table 3 – Non-Federal Organization Requirements

NIST has also developed a Handbook for self-assessment, entitled, *NIST Handbook 162, NIST MEP CYBERSECURITY Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, November 2017. The handbook furthers the requirement for policies, see *Table 4*, by instructing contractors that they need to ensure that security policies are in place, and importantly, that they are understood by employees.

Statement	Document	Page
Ensuring that security policies are in place and understood by company employees. A list of plans and polices companies should have in place is included in Appendix A.	NIST Handbook 162	Page 4

Table 4 - Policies in Place and Understood

One of the common challenges in policy development is that it becomes a paper exercise and does not become part of the corporate culture. Effective security and compliance requires having plans and policies.

Employee awareness and understanding can be accomplished several ways including having employees participate in the development process, including employees in the activities of the plans and policies, providing training (onboarding and ongoing continuous training), and including employees in the testing of plans (e.g. business continuity, disaster recovery, and incident response).

The list referred to in the previous table is shown in detail in *Table 5*.

Plans you should have in place:	Policies and Procedures you should have:
• Business Continuity Plans	• Access Control
• Contingency Plans	• Audit and Accountability
• Continuity of Operations Plans	• Configuration Management
• Critical Infrastructure Plans	• Configuration Planning
• Crisis Communications Plan	• Incident Response

A Requirement for Policies

• Disaster Recovery Plans	• Identification and Authentication
• Incident Response Plan	• Information Flow Control
• Incident Response Testing Plan	• Information Flow Enforcement
• Occupant Emergency Plan	• Information System Maintenance
• Physical/Environmental Protection Plan	• Media Protection
• Plan of Action	• Media Sanitization and Disposal
• Security Assessment Plan	• Mobile Code Implementation
• Security Plan	• Password
• System Security Plan	• Personnel Security
	• Physical and Environmental Protection
	• Portable Media
	• Risk Assessment
	• Security Assessment and Authorization
	• Security Awareness and Training
	• Security Planning
	• Separation of Duties
	• System and Information Integrity
	• System and Services Acquisition
	• System and Communication Protection
	• System Use

Table 5 - Expected Plans and Policies (Minimum)

NIST SP 800-171 & FISMA

Several NIST sources provide further guidance in the critical role that policies have in an information security program. DFARS and NIST efforts to improve the security of unclassified information links the requirement from 800-171 back to the Federal Information Security Management Act (FISMA) of 2002 and this linkage is prescribed in 32 CFR Ch. XX (7–1–17 Edition).

2002.4 Definitions. Subsection (ss) Uncontrolled unclassified information is information that neither the Order nor the authorities governing classified information cover as protected. ***Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.***

A Requirement for Policies

The Computer Security Resource Center at NIST has developed a Frequently Asked Questions (FAQ) page on their website discussion Risk Management for FISMA. One of the questions NIST is frequently asked is whether FISMA compliance is a paperwork exercise. The answer is a resounding NO! NIST further goes on to emphasize the critical role that policies have in building an effective information security program (see adjacent text box).

NIST emphasizes that policies, which document decisions made by management, show a commitment to information security. Using the NIST framework for merely publishing policies is not sufficient, they must be used, evaluated, and refined continuously.

> "Developing sound security policies and procedures is a critical aspect of building an effective information security program. Security policies, while administrative in nature, demonstrate in clear and unequivocal teams, senior management's commitment to information security and protecting the organization's operations (mission, functions, image, and reputation) and assets, individuals, other organizations, and the Nation".

Figure 3 - NIST Statement Re: Security Policies

Making Policies Effective

The intent of the NIST is to ensure that security policies are deployed in a comprehensive way that provides sufficient guidance and a blueprint for information security management and the 110 controls along with Appendix E documented in NIST 800-171. This is consistent with other NIST publications related to NIST 800-171:

Statement	Document	Page
Documenting information security responsibilities is not dependent on the size of the organization. **Even small organizations can prepare a document that states the organizational policy** and identifies the information security responsibilities for a system or for the entire organization.	NIST.SP.800-12	Page 9
Policy controls are addressed by the "-1" controls for every security control family found in NIST SP 800-53. **The "-1" controls establish policy and procedures for the effective implementation** of the selected security control and control enhancement.	NIST.SP.800-12	Page 26
Once again, the more formal the documentation, **the easier it is to enforce and to follow the policy.**	NIST.SP.800-12	Page 31

A Requirement for Policies

Security assurance is a critical aspect in determining the trustworthiness of information systems**. Assurance is the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.**	NIST.SP.800-39	Page 26

Table 6 - NIST's Policy References

Small organizations, if they want to do work with the US Federal Government are required to follow the same guidelines as large organizations. Therefor even small organizations must have security policies. They are also not merely technical solutions or configuring technology settings (configurations). Having an effective security program and effective policies requires them being fully documented, applied, monitored with established performance measures, and be regularly reviewed.

Establishing policies, in the long run, makes the business enterprise, much more efficient and improves security and privacy. NIST 800-53 says that "controls establish policy and procedures for effective implementation. These are foundational, which is why they are also called out for in Appendix E of NIST SP 800-171.

Formalizing policy, as stated in NIST 800-12, makes it easier to enforce and follow the policy. Effective security policies make frequent references to standards and guidelines that exist within an organization, that are to be followed and enforced. If it is not written down it can't be passed along and measured for its effectiveness. Self-audits, or external auditors, would easily identify a significant gap in the information security program that does not have documentation.

Ease of mind, of clients, government clients, or for that matter any clients, is achieved by evaluating the trustworthiness of the information systems. NIST 800-39 articulates that assurance is best achieved if there is some level of "confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy". You cannot have assurance without policies to measure against.

A Requirement for Policies

What Needs to Be Done

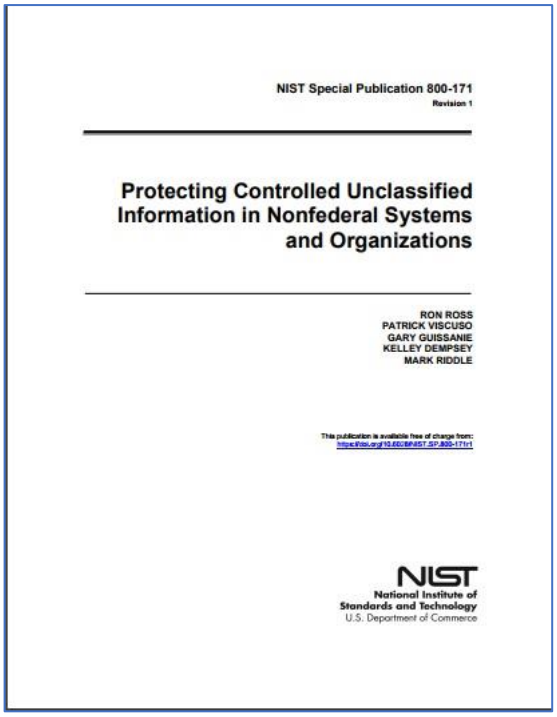

Figure 4 - NIST SP 800-171 Rev1

There are 110 controls in 800-171, and when combined with the requirements of Appendix E, form the foundation of your information security program.

Having policies to address these control requirements as well as establishing baseline Non-Federal Organization policies, procedures, and actions have been well thought out by NIST along with public comment from industry (note: this public comment is open to all) and provide an effective "mechanism" to improve security.

The adequacy of the policies (for security effectiveness and compliance), as well as the determination if the policies are being used/applied is the first step in baselining or reviewing the status and the effectiveness of the policies.

A review must be performed to determine the assurance that the policies are adequate and effective in achieving the firm's objectives for security and compliance. The review can be done on a stand-alone basis or as part of a full and comprehensive review of the security and compliance program.

The review includes an assessment of the overall policy requirements of DFARS and NIST 800-171 and a status of current business enterprise policies. Policies are reviewed for both security and compliance requirements for DFARS. A gap analysis is required to identify potential remediations or improvements that the business enterprise can implement. Once this is complete, and actions are taken to close any gaps, the requirement for policies will be initially achieved. This must be made as part of an annual process so that the business enterprise continues to maintain an effective information security program and remains in compliance.