MEP • MANUFACTURING
EXTENSION PARTNERSHIP®

SUPPLEMENT to the NIST MEP CYBERSECURITY Self-Assessment Handbook

Intended to be used with the NIST MEP Cybersecurity Handbook

to Assist Manufacturers Seeking to Comply with DFARS Cybersecurity Requirements

Disclaimer

The contents of this Supplement are offered as guidance only. NIST and NIST MEP do not make any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this Supplement, or that the use of any information, methods, or processes described in this Supplement may not infringe on privately owned rights; nor assume any liabilities with respect to the use of, or for damages resulting from the use of, any information method or process described in this Supplement. The Supplement does not reflect official views or policy of NIST. Mention of trade names or commercial products does not constitute endorsement or recommendation of use by NIST.

This Supplement has been produced by NIST MEP technical staff and is intended for use by MEP Center staff in conjunction with the NIST MEP Cybersecurity Self-Assessment Handbook (http://tinyurl.com/cybersecurity-assess-handbook) specifically to assist U.S. manufacturers who supply products within supply chains for the DOD and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with DFARS clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”.

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

This Supplement includes mention of official DOD policies and regulations that are part of the aforementioned DFARS clause. Such mention is public domain information and does not constitute any policy statements or regulatory enforcement by NIST.

NIST is a non-regulatory agency of the U.S. Department of Commerce; as such, NIST makes no claims that use of this Handbook will satisfy the regulatory requirements of DOD in conjunction with DFARS. Compliance with the DFARS can only be satisfied through approval by the DOD in conjunction with official DFARS requirements. All matters relating to the DFARS should be directed to the DOD in conjunction with the requirements of DFARS clause 252.204-7012. Additional information about the DFARS can be obtained at

http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf

Introduction

This Supplement to the Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in response to DFARS Cybersecurity Requirements provides additional guidance to be used with the Handbook. This Supplement focuses on information needed by manufacturers who are seeking to comply with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting.”

This Supplement should be used in conjunction with the subject Handbook, which provides a step-by-step guide to assessing a small manufacturer’s information system against the security requirements in NIST SP 800-171 rev 1 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

This Supplement provides useful information about the DFARS cybersecurity requirements, along with a 3-step process that manufacturers can follow to assist in their path toward compliance with DFARS.

What is DFARS requirement?

Clause 252.204-7012 of the DFARS requires defense contractors and subcontractors to do the following:

1. Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor’s internal information system or network
2. Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor’s ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DOD Cyber Crime CenterIf requested, submit media and additional information to support damage assessment
4. If requested, submit media and additional information to support damage assessment
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information

For specific details about cybersecurity requirements within DFARS clause 252.204-7012, users of this Supplement should refer to the DFARS clause, as well as the Frequently Asked Questions and other information that has been published by the DOD and that is available at http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

What is the purpose of DFARS clause 252.204-7012?

DFARS clause 252.204-7012 was structured to ensure that controlled unclassified DOD information residing on a contractor’s internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes. In addition, by providing a single DOD-wide approach to safeguarding covered contractor information systems, the clause prevents the proliferation and safeguarding of controlled unclassified information clauses and contract language by the various entities across DOD.

What is “adequate security”?

The DFARS requires that contractors and their subcontractors employ “adequate security.” This means that protective measures are employed that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. Contractors should implement, at a minimum, the security requirements in National Institute of Standards and Technology Special Publication 800-171 rev 1, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.” Contractors are obligated to rapidly report (within 72 hours of discovery) any cyber incident that affect the covered contractor’s information system, covered defense information, or the contractor’s ability to provide operationally critical support. In addition, the reporting obligations require that contractors isolate and capture, if possible, an image of the malicious software (e.g., worm, virus, etc.) and provide access to covered contractor information systems and other information if requested by the DOD.

What is a “Covered contractor information system”?

DFARS 252.204-7012(a) defines “covered contractor information system” as “an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.” A covered contractor information system is specifically an ‘‘unclassified’’ information system. A covered contractor information system requires safeguarding in accordance with 252.204-7012(b) because performance of the contract requires that the system process, store, or transmit covered defense information.

When and how should DFARS clause 252.204-7012 flow down to subcontractors?

DFARS clause 252.204-7012 flows down to subcontractors without alteration, except to identify the parties, when performance will involve operationally critical support or covered defense information. Per 252.204-7012(m)(1), the prime contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information, thus necessitating flow-down of the clause. You should consult with your contracting officer if clarification is required. The DoD’s emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flow down of information requiring protection.

Flow down is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor to be in compliance with these terms. If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not be on that subcontractor’s information system.

When is DFARS clause 252.204-7012 required in contracts?

DFARS clause 252.204-7012 is required in all solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for the acquisition of commercial items. The clause is not required for solicitations and contracts solely for the acquisition of Commercial Off the Shelf (COTS) items. COTS is a commercial item that has been sold in the commercial marketplace in substantial quantities, and is offered to the government in a contract or subcontract without modification. Procurements solely for the acquisition of COTS items are extremely unlikely to involve covered defense information or operationally critical support.

Commercial items include COTS and other commercial items that are or are about to be available in the marketplace. These products can also be modified to meet Government requirements. If a commercial item must be modified to meet Government requirements, such modifications may require the use and safeguarding of covered defense information, or the resulting service could be operationally critical for DoD. When the acquisition of commercial items involves covered defense information, such as in some cases when commercial items, services, or offerings are tailored to meet a customer’s requirement, DFARS clause 252.204-7012 will apply to commercial items involving covered defense information.

The clause is not required to be applied retroactively, but that does not preclude a contracting officer from modifying an existing contract to add the clause.

What does this DFARS cybersecurity requirement mean?

This requirement is an “included clause” in defense contracts. By signing a defense contract, the contractor agrees to comply with the contract terms. DFARS 252.204.7012 applies to information systems that process, store, or transmit Controlled Unclassified Information (CUI) provided by or developed for the DoD. CUI is information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Executive Order 13556 “Controlled Unclassified Information” (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to its Information Security Oversight Office (ISOO).

32 CFR Part 2002 “Controlled Unclassified Information” was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI – or which operate, use, or have access to Federal information and information systems on behalf of an agency.

Examples of CUI include: Controlled Technical Information, Export Control Information, and DoD Critical Infrastructure Security Information.

Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Export control information could include 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.

DoD Critical Infrastructure Security Information could include information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.

For additional information visit the National Archives CUI webpage: https://www.archives.gov/cui

What do contractors need to do to ensure compliance and when does this apply?

Defense contractors are **REQUIRED** by DFARS to provide adequate security on all covered contractor information systems. To provide adequate security, defense contractors must implement, at a minimum, the following information security protections: NIST SP 800-171, as soon as practical, but ***not later than December 31, 2017***.

What is NIST SP 800-171 and how does a manufacturer implement it?

NIST Special Publication 800-171 was developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 USC § 3541 et seq., Public Law (P.L.) 113-283. The publication is titled, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," NIST SP 800-171 Revision 1, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

NIST SP 800-171 provides federal agencies with recommended requirements for protecting the confidentiality of controlled unclassified information (CUI):

1. when the CUI is resident in nonfederal information systems and organizations;
2. when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
3. where 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 CUI Registry.

NIST SP 800-171 requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. A nonfederal information system is a system that does not meet the criteria for a federal system.

The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This includes the DOD and is resident within DFARS clauses that apply to defense contracts.

For ease of use, the NIST SP 800-171 security requirements are organized into 14 families. The Self- Assessment Handbook is organized based on these 14 families.

For each family, a brief overview is provided. Table 1 below lists the security requirement families addressed in the Handbook.

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	Systems and Communications Protection
Maintenance	System and Information Integrity

Table 1. NIST SP 800-171 Security Requirement Families

The security requirement with the original numbering scheme from 800-171 is listed throughout the Handbook.

NIST SP 800-171 assumes that small manufacturers currently have IT infrastructures in place, and it is not necessary to develop or acquire new systems to handle CUI. Most small manufacturers have security measures to protect their information which may also satisfy the 800-171 security requirements. A variety of potential security solutions can be implemented to satisfy the security requirements. There is no single security solution, each small manufacturer will need to understand their operating environment and apply the security requirements to meet their situation. Small manufacturers may not have the necessary organizational structure or resources to satisfy every security requirement. It is perfectly acceptable to implement alternative, but equally effective, security measures to satisfy a security requirement.

NIST MEP Three Step Approach to Adequate Cybersecurity and Complying with DFARS

NIST MEP has developed a Three Step Approach to assessing information systems against the security requirements in NIST SP 800-171 and working toward the demonstration of compliance to the DFARS.

The outputs of the Three Step Approach will provide the evidence to demonstrate compliance with the DFARS. Full compliance is only achieved when the DoD Contracting Officer or Prime Contractor have fully reviewed and approved the Three Step Approach outputs.

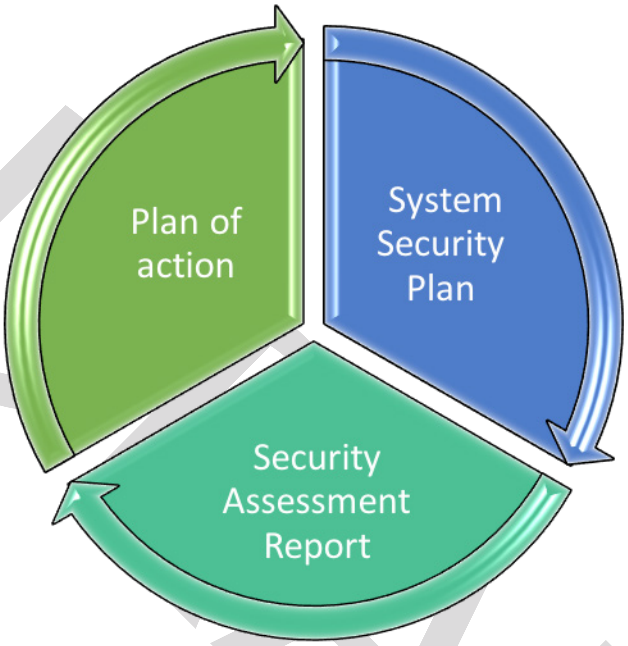

Figure 1. Three Step Approach to Adequate Cybersecurity

STEP 1 | DEVELOP A SYSTEM SECURITY PLAN

Manufacturers should develop a system security plan, which describes how the 800-171 security requirements are met or how the company plans to meet the requirements. The system security plan describes:

- the system boundary;
- the operational environment;
- how the security requirements are implemented; and
- the relationships with or connections to other systems.

Companies should develop plans of action that fully describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Companies can document the system security plan and plan of action as separate or combined documents and in any chosen format.

The System Security Plan required by 800-171 (requirement 3.12.4), and any associated plans of action connected to that system security plan, are the mechanisms to provide evidence that demonstrate implementation of NIST SP 800-171.

Once the Systems Security Plan has been developed, it should be submitted to the DoD Contracting Officer or Prime contractor for review and approval, along with the Security Assessment Report and Plan of Action (Steps 2 and 3). In some cases, the DoD Contracting Officer may request review by the DoD Chief Information Officer (CIO). The DOD CIO may need clarification or additional information before granting final approval.

A question frequently asked by companies is ‘how do I know that what I’ve done meets the NIST SP 800-171 requirement?” If there is any concern, a company can include that portion of the system security plan with its technical proposal. The System Security Plan should describe how security requirements are implemented. Elements of the system security plan may also inform a discussion of risk between the contractor and requiring activity/program office.

The System Security Plan should also be used to identify situations where elements of the NIST SP 800□171 requirements cannot practically be applied, or when events result in short- or long-term issues that must be addressed by assessing risk and applying mitigations. The System Security Plan is used to describe any exceptions to the requirements to accommodate special circumstances (e.g., medical devices), any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability per NIST SP 800-171 security requirements 3.11.1 and 3.12.1, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities.

STEP 2 | CONDUCT THE ASSESSMENT AND PRODUCE A SECURITY ASSESSMENT REPORT

Manufacturers should develop a plan for conducting the security requirements assessment and follow

their plan to conduct the assessment of their system against the security requirements in SP 800-171. The Handbook provides a step-by-step guide to assessing a manufacturer’s information system against the security requirements in NIST SP 800-171.

The results of the security control assessments are documented in Security Assessment Report Security Assessment Reports include information from assessors necessary to determine the effectiveness of the security employed in the information system. The Security Assessment Report provides important information to company management on determining cybersecurity risks.

Companies may choose to develop an assessment summary from the detailed findings that are generated by assessors during the security control assessments. An assessment summary can provide an abbreviated version of a Security Assessment Report focusing on the highlights of the assessment, synopsis of key findings, and recommendations for addressing weaknesses and deficiencies in the security assessed.

The results of security control assessments ultimately influence security control implementations, the content of security plans, and the respective plans of action.

STEP 3 | PRODUCE A PLAN OF ACTION

Once the assessment has been completed and the Security Assessment Report developed, assessor findings should be reviewed and the risk of noted weaknesses and deficiencies evaluated. Company management should review the effectiveness of the security requirements and determine/initiate appropriate response actions. The Plan of Action should be developed or updated in the case of repeat assessments. Based on the Plan of Action, the System Security Plans may need to be reviewed and updated.

A small manufacturer should develop plans of action that describe how any unimplemented security requirements will be met and how any planned improvements will be implemented. The Plan of Action should include detailed milestones used to measure progress.

Companies can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Once the Systems Security Plan, Security Assessment Report and Plan of Action have been developed, they should be submitted to the DoD Contracting Officer or Prime contractor for review and approval. In some cases, the DoD Contracting Officer may request review by the DoD Chief Information Officer (CIO). The DoD CIO may need clarification or additional information before granting final approval.

MEP • MANUFACTURING
EXTENSION PARTNERSHIP®

National Institute of
Standards and Technology
U.S. Department of Commerce

100 Bureau Drive M/S 4800, Gaithersburg, MD 20899 | www.nist.gov/mep | PH:(301) 975-5020 | FX:(301) 963-6556 | mfg@nist.gov