DFARS, NIST, and Incident Reporting

Page Contents

Jump to...

FARS, NIST, and Incident Reporting

e

DISCLAIMER: The information below is provided as a convenience to our visitors to this site. It should not be used as a legal opinion of the DFARS regulations.

Guidance for Procurements requiring implementation of NIST SP 800-171

DoD has drafted guidance for procurements requiring implementation of NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and is making the draft guidance available to the public. The supporting documents are very interesting as they provide additional guidance on individual controls. The document can be found here.

Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73, etc

On April 2, 2018 DoD published this document below to address FAQs from January 27, 2017. The answers to the questions start on page 13 of the document: Cyber DFARS FAQs.

DPAP Guidance for Acquisition Personnel

On September 17, 2017, the DPAP provide this document as guidance on the DFARS and implementing NIST 800-171 within your organization. It has some clarifying language on the use of the SSP and POAM.

What is NIST SP 800-171?

The standard from NIST provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

- when the CUI is resident in non-federal information systems and organizations.
- 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.
- where there are no specific safeguarding requirements for protecting the confidentiality of CUI.

SP 800-171 guidelines are tailored for the non-federal information systems that contractors already have in place, with a goal of attempting to avoid requiring contractors to completely replace legacy information systems.

Where can I find the NIST 800-171 document?

NIST Special Publication 800-171 R1, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” December 2016, is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf .

SP 800-171A - a guide for assessing NIST 800-171 controls

Feb 26, 2017: NIST announces the release of the Final Draft of Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information. This publication is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in NIST 800-171.

SP 800-171A provides a consistent process for assessment and additional explanation of the cyber requirements for each of the 110 requirements. Each control is accompanied by a statement of “Assessment Objective,” discussion of “Potential Assessment Methods and Objects,” and reference to “Supplemental Guidance”. This is a very useful document to provide much more detail for each control.

Cyber DFARS: Key Questions, Asked & Answered by Robert Metzger

The two documents below (Key Questions, Asked & Answered, Part 1 and Part 2) have been provided by Robert Metzger, an attorney in private practice who specializes in cybersecurity and government contracts. He addresses a number of common questions concerning the DFARS and SP 800-171.

Oct 20 2017 DFARS_QA_Part_I.pdf Oct 27 2017 DFARS_QA_Part_II.pdf

What is the purpose of the DFARS clause 252.204-7012?

“DFARS clause 252.204-7012 was structured to ensure that 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 of non-harmonized cyber security clauses and contract language by the various entities across the DoD.” *

What is CDI?

See http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm. The four types of CDI (DFARS 204.7301 (Definitions)):

- controlled technical information (CTI) (with military or space application)
- critical information (operations security)
- export controlled information
- ‘‘[a]ny other information’’ that requires safeguarding or dissemination controls pursuant to ‘‘laws, regulations, and government-wide policies”.

The first of these types, “controlled technical information,” corresponds to what was controlled as “Unclassified Controlled Technical Information” (UCTI) under an earlier regulation “Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information,” (DFARS Case 2011-D039), Final rule, 78 Fed. Reg. 69273 (Nov. 18, 2013).

What is CTI?

Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled Technical Information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). 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. *

CUI vs. UCTI vs. CDI

NIST 800-171 refers to “Controlled Unclassified Information” (CUI) and was dated before the new rules were put in place. “Unclassified Controlled Technical Information” (UCTI) was the original term in DFARS 252.204-7012. “Covered Defense Information” (CDI) is the new term that encompasses all of the above, as well as new types of information.

What does this DFARS mean for my business?

Every contractor that takes a contract with this DFARS is subject to an immediate requirement to provide “adequate security” for CDI and contractors must report “cyber incidents” within 72 hours of discovery (DFARS 252.204-7012(b)). In addition, a company that receives a contract subject to the new DFARS must report to the DoD Chief Information Officer (CIO) – within 30 days of contract award – any security requirement specified by SP 800-171 “not implemented at the time of contract award” (DFARS 252.204-7012(b)(2)(ii)(A)). *

What are the flowdown requirements?

DFARS clause 252.204-7012 defines the requirement that contractors are required to flowdown the substance of the clause in all its subcontracts (including for commercial items) where their efforts will involve covered defense information or where they will provide operationally critical support. Contractors must require subcontractors to rapidly report cyber incidents directly to DoD via http://dibnet.dod.mil and to any higher tier contractor (including the prime).

“DFARS clause 252.204-7012 flows down to subcontractors without alteration when performance will involve operationally critical support or CDI. The contractor should consult with the contracting officer when it is uncertain if the clause should flowdown. Flowdown is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the terms of clause 252.204-7012 then CDI should not be on that subcontractor’s information system.” *

What is the date for implementing NIST SP 800-171?

"252.204-702 (ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award."*

If suppliers are NIST SP 800-53 compliant, can they use that fact to demonstrate compliance with NIST 800-171?

This is a difficult question to answer as it depends:

1. NIST 800-53 has controls, but the mechanisms vary by the risk level that you have associated with the information system that needs to be protected.
2. NIST 800-171 is derived from 800-53 and specifies the risk level as Moderate (the three risk levels are: High, Moderate and Low)
3. If a supplier believes they are compliant with NIST 800-53 Moderate or above, they most probably can show compliance to NIST 800-171, but it is not guaranteed (example: 800-171 controls are derived, but NIST have identified specific requirements in 800-171, such as 2FA for network access for normal users, and 800-53 does not go to that level of prescription.

Cyber Incident Reporting

Introduction

252.204-7012 requires cyber incident reporting when a contractor or subcontractor discovers that actions taken through the use of computer networks have resulted in a compromise or an actual or potentially adverse effect on a covered IT system and/or the covered defense information residing within that covered IT system. The regulation provides a detailed process for investigating and reporting the cyber incident to the DoD and the prime contractor (or next higher-tier subcontractor). In order to report cyber incidents, DoD contractors if they have not already done so, must obtain a DoD-approved medium assurance certificate.

This site shows the relationship of certificates: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx.

Your medium assurance certificate will need to be accessible by the browser you will use to report an incident, otherwise you cannot get access into the incident report form. It is suggested you obtain the certificate before an incident that needs reporting, as the requisite identity verification process can take a while depending upon your organization structure.

NOTE from Exostar: If you have Exostar MLOA hardware (HW) certificates from FIS, they are eligible for DIBNet incident reporting.

How do we report?

The text below is an abstract from: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(Exostar note: a snippet of the report process is shown below and you need to have all the information ready at hand to complete the form.)

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx .

Article on incident reporting

Here is an article by Bob Metzger, "Incident Reporting Key to New Cybersecurity Rule" concerning incident reporting that provides an indepent review of the requirement.
How useful was this content?

Your Rating: Results: 21 rates