DFARS 252.204-7012,
Safeguarding Covered Defense Information and Cyber Incident Reporting

UPDATE

Vicki Michetti, DoD CIO, Director, DIB Cybersecurity Program

Mary Thomas, OUSD(AT&L), Defense Procurement and Acquisition Policy

Defense Contract Management Agency (DCMA) Oversight of DFARS Clause 252.204-7012

- **DCMA role is consistent with model upon which all clauses are based – at time of contract award, contractor self-attests compliance**
- **Actions DCMA will take in regards to cyber-security are:**
  - **Verify that system security plan and any associated plans of action are in place (DCMA will not assess SSP against NIST 800-171 requirements)**
  - **If potential cyber-security issue is detected - notify contractor, DoD program office, and DoD CIO**
  - **During the normal Contract Receipt and Review process - verify that applicable cyber-security clauses are in contract**
  - **Through Oct 2017 - verify that contractor submitted to DoD CIO notification of security requirements not yet implemented**
  - **Verify contractor possesses medium assurance certificate as required to report cyber incidents**
  - **As may be required – facilitate entry of government external assessment team into contractor facilities via coordination with cognizant government and contractor stakeholders**

NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

- **Developed for use on contractor and other nonfederal information systems to protect CUI *(Revision 1 published December 2016)***
  - **Replaces use of selected security controls from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**
- **Enables contractors to comply using systems and practices likely already in place**
  - **Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.**
- **Provides standardized/uniform set of requirements for all CUI security needs**
  - **Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers)**
  - **Allows contractor to implement alternative, but equally effective, security measures to satisfy CUI security requirements**

An Approach to Implementing NIST SP 800-171

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware. For companies new to the requirements, a reasonable approach would be to:

1. **Examine each of the requirements to determine**
   - **Policy or process requirements**
   - **Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)**
   - **IT configuration requirements**
   - **Any additional software or hardware required**

   Note that the complexity of the company IT system may determine whether additional software or tools are required.
2. **Determine which of requirements can readily be accomplished by in-house IT personnel and which require additional research**
3. **Develop a plan of action and milestones to implement the requirements.**

Cybersecurity Evaluation Tool (CSET) Tool

- **CSET is a no cost application developed by the DHS's Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT)**
  - **The tool provides a systematic approach for evaluating an organization's security posture by guiding asset owners and operators through a step-by-step process to evaluate their industrial control system and information technology network security practices.**
  - **To use the assessment tool, users select one or more government and industry recognized cybersecurity standards, including NIST SP 800-171. CSET then generates questions that are specific to those requirements and presents the assessment results in both summary and detailed form.**

- **Download at https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET or to request a physical copy of the software, contact cset@dhs.gov**
- **Select "Advanced Mode" which will provide the option to select NIST 800-171**

Frequently Asked Questions — "Compliance" with DFARS Clause 252.204-7012

Q: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A: The DFARS rule did not add any unique/additional requirement for the Government to monitor contractor implementation of required security requirements.

Q: Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?

A: The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. Nor will DoD recognize 3rd party assessments or certifications. By signing the contract, the contractor agrees to comply with the terms of the contract.

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Security Requirement 3.12.4 – System Security Plan (SSP)

3.12.4 — Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems.

- **The System Security Plan (SSP) should be used to document:**
  - **How the requirements are met or how organizations plan to meet requirements**
    - **3.12.2 addresses plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities**
  - **Situations where requirements cannot practically be applied (non-applicable)**
  - **DoD CIO approved alternative but equally effective security measures**
  - **Exceptions to accommodate special circumstances (e.g., CNC machines and/or shop floor machines)**
  - **Individual, isolated or temporary deficiencies addressed by assessing risk and applying mitigations**

- **When requested by the requiring activity, the SSP (or elements of the SSP) and any associated plans of action, should be submitted to the requiring activity/contracting officer to demonstrate implementation of NIST SP 800-171.**

Procurement Technical Assistance Program (PTAP)

- **The Procurement Technical Assistance Program (PTAP), administered by DLA's Office of Small Business in cooperation with states, local governments and nonprofit organizations, was established to expand the number of businesses capable of participating in government contracts.**
- **Under the program, Procurement Technical Assistance Centers (PTACs) help businesses pursue and perform under contracts with the DoD, other federal agencies, state and local governments and with government prime contractors. Most assistance is free.**
  - **Many PTACs are affiliated with Small Business Development Centers and other small business programs, and form a nationwide network of counselors across all 50 states, Washington, D.C., Puerto Rico and Guam.**
  - **Other PTACs specialize in assistance to federally recognized Indian tribes and Alaska Native entities throughout the country**
- **We are working to provide the PTAC counselors with information for small businesses who seek their assistance on the implementation if DoD's cybersecurity regulations.**

Subcontractor Flowdown

The Department's emphasis is on managing and when possible, limiting, the flow down of information requiring protection.

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

- **The clause flows down to subcontractors when performance will involve operationally critical support or CDI**
- **The contractor will determine if – and may consult with the contracting officer if necessary – the information required for subcontractor performance retains its identify as CDI and requires safeguarding or dissemination controls**
- **Flowdown is to be enforced by the prime contractor. If a subcontractor does not agree to comply with the clause, CDI should not be on that subcontractor's information system.**

Resources

- **Frequently Asked Questions (FAQs)**
  http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf
- **NIST Special Publication 800-171 Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
- **DHS Cybersecurity Evaluation Tool (CSET) Tool**
  - **Instructions to download/install:** https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
  - **Factsheet:** https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf
- **Procurement Technical Assistance Program (PTAP)**
  http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx
- **Questions? Submit questions via email at** osd.dibcsia@mail.mil

Resources - Industry Information Day

DoD is hosting an "Industry Information Day" to present a briefing, and receive/address industry feedback on the implementation of DFARS Case 2013–D018, "Network Penetration Reporting & Contracting for Cloud Services"

- **The public meeting will be held on Friday, June 23, 2017, from 9:00 a.m. to 1:00 p.m., at the Mark Center Auditorium, Alexandria, VA**
- **Individuals wishing to attend the public meeting should register by Monday, June 12, 2017by Monday, June 12, 2017**
- **Questions should be sent by email to OSD.DIBCSIAEvents@mail.mil with the subject line of the email stating, "Industry Information Day"**
- **Questions should be submitted by June 2, 2017 for consideration**

Federal Register Notice (FRN) at
https://www.gpo.gov/fdsys/pkg/FR-2017-04-28/pdf/2017-08589.pdf