Government Contractors Forum

DFARS 252.204-7012:
Life After December 31, 2017
Panelists

Moderator

Gunjan Talati, Government Contracts Partner at Kilpatrick Townsend

Panelists

Vicki Michetti, Director of the Defense Industrial Base (DIB) Cyber Security (DIB CS) Program office, under the DoD Chief Information Officer

Mary Thomas, Program Analyst for the Director of Defense Procurement and Acquisition Policy (DPAP), in the Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)

Sandeep Kathuria, Corporate Counsel at Northrop Grumman
DoD Clause – Final Rule Issued October 21, 2016

Contractors and subcontractors must:

• provide “adequate security” for “all covered defense information”
• in accordance with NIST 800-171
• rapidly report breaches to the agency
• perform specific actions in response to a breach
• engage in forensic preservation (media and malware)
Who Cares About DFARS 252.204-7012 Anyway?

• Applicability is for Department of Defense contracts AND subcontracts

• Does not apply to COTS solicitations

• Applies to cloud service providers
• DoD’s definition of “covered defense information” includes:
  – unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—
    (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
    (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
Determining Whether There’s CDI:
  • Contract Appendices
  • Marking/Legends on Documents
  • If it originates with DoD, should not have to guess

But what about CDI the Contractor gets from third parties or the Contractor *generates*?
  • NARA website
  • Context Clues
  • Open communication with DoD/contracting activity
  • When in doubt - ?
DFARS 252.204-7012: What’s Covered?

• Systems “operated on behalf of the Government” subject to “security requirements specified elsewhere in the [DoD Contract]”

• Systems not operated on behalf of the Government subject to NIST 800-171
DFARS 252.204-7012: What’s Covered?

- Determining security requirements: are you operating a system “on behalf of” the Agency?
  - “On or behalf of the Government” – not defined
  - Open to Interpretation
  - Context clues:
    - Are you supplying the Government services?
    - What kind of services?
    - Using who’s equipment?
    - At who’s location?
    - Who’s logging on to who’s system?
• Practical Concerns:
  
  – What if you’re unsure if you’re providing services on behalf of DoD?
  
  – What if you’re providing services on behalf of DoD but CDI never enters your equipment or systems?
    
    • What measures do you have in place to ensure CDI stays off your system?
  
  – What if your DoD contract lists both 252.204-7012 and 252.239-7010? Do you need to comply with both?
NIST SP 800-171

- NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations (*June 2015, Revision 1 December 2016*):
  - Recommended requirements for protecting the confidentiality of CUI when
    - CUI is resident in nonfederal information systems/organizations
  - Information systems where the CUI resides are **not used or operated** by contractors of federal agencies or other organizations on behalf of those agencies
NIST 800-171 – THE DEADLINE:

• DoD Contractors subject to NIST 800-171 were required to implement those controls on or before December 31, 2017.

• But 12/31/17 was not the end!
  – Must maintain ongoing compliance efforts
NIST 800-171 Variance Procedure:

- Back-up: Do you need a variance?
  - Consider that the control may not apply to your systems or the services you are performing for DoD.
    - Still must advise DoD
  - Consider whether you’re actually going to handle CDI.
  - Consider whether you can solve the problem by segregating or re-locating the data to a different part of your network.
  - Consider that you may actually comply.
    - Under some circumstances one 171 control-in-place may satisfy multiple controls.
    - Depending on circumstances, DoD may consider written policies in place as sufficient as long as they meaningfully address the concern behind the control.
Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

- NIST SP 800-171 was revised (Revision 1) in December 2016 to enable nonfederal organizations to demonstrate implementation or planned implementation of the security requirements with a “system security plan” and associated “plans of action”
Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

• Security requirement 3.12.4 (System Security Plan) requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

• Security Requirement 3.12.2 (Plans of Action) requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.
DoD Cyber Incident Reporting:

• “Rapid” (within 72 hours) of “discovery of any cyber incident”

• Centralized website: https://dibnet.dod.mil

• Need a “medium assurance certificate”

• Forensic mindset: preserve affected data and media
https://dibnet.dod.mil
### What to report?

#### DoD Contractors

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident.

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contact or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information
Additional DoD Requirements: When the Contractor discovers a cyber incident that affects covered information or system, the Contractor “shall” –

a) Conduct a review for evidence of compromise of covered defense information . . .

d) Submit identified malicious software in accordance with instructions provided by the Contracting Officer.

e) Preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

f) Provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis
Comply and Cooperate, but protect your own systems and data:

- **Image and backup** everything you provide DoD
- **Mark** your attributional and proprietary information to protect from disclosure during incident investigation.
- **Safeguard** other client information that may reside on your systems (they had nothing to do with this!)
- **Know** your legal rights and hire a lawyer, forensic expert early in the process
Cloud Services and Solutions

• DFARS Clause 252.239-7010 — Cloud Computing Services

• Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud

• Requires the cloud service provider to:
  – Comply with the DoD Cloud Computing Security Requirements Guide
  – Comply with requirements for cyber incident reporting and damage assessment
Cloud Services and Solutions

• **DFARS Clause 252.204-7012 — Safeguarding Covered Defense Information and Cyber Incident Reporting**

• Applies when a contractor intends to use an external cloud service provider to store, process, or transmit Covered Defense Information in the performance of a contract

• Ensures that the cloud service provider:
  – Meets requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline
  – Complies with requirements for cyber incident reporting and damage assessment
When should DFARS Clause 252.204-7012 flow down to subcontractors?

- The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information.
- The contractor shall determine if the information required for subcontractor performance is, or retains its identify as, covered defense information and requires safeguarding.
- Flowdown is a requirement of the terms of the contract with the Government, which must 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 DFARS Clause 252.204-7012, then covered defense information shall not be shared with the subcontractor or otherwise reside on its information system.
DFARS 252.204-7012: Make Me Comply!

- Contractual remedies
  - Termination for default
- Adverse past performance
- Suspension/Debarment
- Civil suit exposure
DFARS 252.204-7012: Let’s Comply!

- Have a DFARS 252.204-7012 compliance plan in place
- Identify clause in your contract
- Identify systems you’ll use to perform
- Determine whether you, subs, CSPs, encounter CDI
- Identify security controls, reporting and other obligations and flow-down to subs
- Discuss questions, work through issues with CO and DoD
- Timely submit notices of non-compliance, requests for variance.

YOUR OBLIGATIONS DIDN’T END ON 12/31/2017!
Implementing NIST SP 800-171 – Where to Get Assistance

- **NIST Manufacturing Extension Partnership (MEP)**
  - Public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers
  - DRAFT Cybersecurity Self-Assessment Workbook for Assessing NIST SP 800-171 Security Requirements and Complying with DFARS Cybersecurity Requirements released to MEP Centers October 2017

- **Procurement Technical Assistance Program (PTAP) and Procurement Technical Assistance Centers (PTACs)**
  - Nationwide network of centers/counselors experienced in government contracting, many of which are affiliated with Small Business Development Centers and other small business programs

- **Cybersecurity Evaluation Tool (CSET)**

- **No-cost application, developed by DHS’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control system and information technology network security practices**
Help!

Resources

- DPAP Website [http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html](http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) for DFARs, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- Cybersecurity Evaluation Tool (CSET) - Download at [https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET](https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET) or request physical copy of software at cset@dhs.gov — Select “Advanced Mode” to display option to select NIST 800-171
- Questions? Submit via email at osd.dibcsia@mail.mil
Contact Us

**Vicki Michetti**
Director, DIB Cybersecurity Program
DoD CIO
[vicki.d.michetti.civ@mail.mil](mailto:vicki.d.michetti.civ@mail.mil)

**Sandeep Kathuria**
Corporate Counsel
Northrop Grumman
[Sandeep.Kathuria@ngc.com](mailto:Sandeep.Kathuria@ngc.com)

**Mary Thomas**
OUSD (AT&L)
Defense Procurement & Acquisition Policy
[mary.s.thomas.civ@mail.mil](mailto:mary.s.thomas.civ@mail.mil)

**Gunjan Talati**
Partner, Government Contracts
Kilpatrick Townsend & Stockton LLP
[gtalati@kilpatricktownsend.com](mailto:gtalati@kilpatricktownsend.com)