Procurement Division Meeting: Compliance Under 252.204-7012

January 9, 2018

Susan Warshaw Ebner
Fortney & Scott, LLC
1750 K Street, NW, Suite 325,
Washington, DC 20006
www.fortneyscott.com

Rolando Sanchez
1629 K Street, NW, Suite 300
Washington, DC 20006
www.sanchezpllc.com
rolando@sanchezpllc.com

Agenda

- Overview of Department of Defense ("DoD") FAR Supplement ("DFARS") Safeguarding Covered Defense Information and Cyber Incident Reporting
- Overview of Follow-on Guidance
- Some Legal Implications to Consider
- What Are The Next Steps?

DFARS Safeguarding and Reporting Rule

- **DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**
  - The DFARS defines a number of terms:

    - "Adequate security"
    - "Compromise"
    - "Contractor attributional / proprietary information"
    - "Controlled technical information"
    - "Covered contractor information"
    - "Covered defense information"
    - "Cyber incident"
    - "Forensic analysis"
    - "Malicious software"
    - "Media"
    - "Operationally critical support"
    - "Technical information"

DFARS Safeguarding and Reporting Rule

- What Does the Rule Require:
  - Contractor is required to provide "***adequate security*** on **all covered contractor information systems**", including compliance with NIST SP 800-171, and
  - Contractor is required to ***rapidly report*** within 72 hours of any actual or suspected "**cyber incident**"
- Applies To All DoD procurements, including Commercial Items except for those solely for the acquisition of COTS items
- Contractor must still comply with other DOD and non-DOD requirements governing the protection of information
  - This rule is in addition to any applicable NISPOM requirements

DFARS Safeguarding and Reporting Rule

- Rule Implementation as of December 31, 2017
  - Requires implementation of the version of clause in your contract, or as authorized by Contracting Officer
  - For contracts awarded prior to October 1, 2017, current version requires contractors to notify the DOD CIO ***within 30 days of contract award*** of security requirements not implemented
  - Security requirements **shall** be implemented **by December 31, 2017**
- **Limited Exceptions** To Application of NIST SP 800-171:
  - When there is a written request to vary from **NIST SP 800-171,** and
  - "an authorized representative" from DoD CIO adjudicates that:
    - The security requirement is inapplicable, ***or***
    - There is an alternative, but equally effective, security measure in place

DFARS Safeguarding and Reporting Rule

- WRINKLE: Where contractor uses external cloud service provider (CSP) “to store, process, or transmit any covered defense information in performance” of the contract, the CSP compliance requirement is limited:
  - CSP must MEET equivalent security requirements to FedRAMP Moderate baseline
  - CSP must COMPLY with five DFARS clause provisions that require:
    - Cyber incident reporting,
    - Malicious software detection and isolation,
    - Media preservation and protection,
    - Government access to additional information, and equipment necessary for forensic analysis, if requested, and
    - Cyber incident damage assessment
  - If contractor is a CSP, then it must comply with all parts of -7012.

DFARS Safeguarding and Reporting Rule

- **NIST SP 800-171 requires compliance with 110 Security Requirements to form a minimum level of CUI protection:**
  - The 110 Security Requirements Are Divided Into 14 Families Of Requirements:

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

DFARS Safeguarding and Reporting Rule

- **Examples of NIST 800-171 Security Requirements:**

  - **3.1.12:** Monitor and control remote access sessions
  - **3.1.16:** Authorize wireless access prior to allowing such connections
  - **3.4.9:** Control and monitor user-installed software
  - **3.5.8:** Prohibit password reuse for a specified number of generations
  - **3.10.4:** Maintain logs of physical access
  - **3.12.2:** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems

DFARS Safeguarding and Reporting Rule

- **Rule Contains A Cyber Incident Reporting Requirement:**
  - Requires you to identify if you have a reportable "cyber incident"
  - If a "cyber incident occurs", you are required to
    - Rapidly Report to DoD within 72 hours of actual or suspected cyber incident (http://dibnet.dod.mil).
    - Provide the DoD Cyber Crime Center (DC3) with the "malicious software, if detected and isolated"
    - Engage in media preservation and protection for at least 90 days for all known affected information systems
    - See also DFARS 204.73 – "A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause . . ."

DFARS Safeguarding and Reporting Rule

What to Report:

- Company name
- Company POC
- DUNS Number
- Contract number(s)
- Contracting Officer POC
- USG Program Manager POC
- Contract clearance level
- Facility CAGE code
- Facility Clearance Level
- Impact to CDI
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- Ability to provide operationally critical support
- DoD programs, platforms or systems involved
- Type of compromise
- Description of technique or method used in cyber incident
- Incident outcome
- Incident/Compromise narrative
- Any additional information

DFARS Safeguarding and Reporting Rule

- **Cyber Incident Reporting Requirement (continued):**
  - Conduct cyber incident damage assessment activities
  - Upon DOD request, provide media or access to covered information systems and equipment
  - Report to other Government locations as directed
  - Other reports as required (e.g., export control disclosures)
- Don’t Forget To Mark Your Data
  - Mark Government data consistent with requirements
  - ***Mark Your OWN Data to protect and preserve your rights***

DFARS Safeguarding and Reporting Rule

- You Must Flow Down To All Tiers:
  - Flow down to your “subcontractors” and “similar contractual instrument” holders
  - Includes flow down to subcontracts for Commercial Items
  - If the subcontracts/agreements provide “operationally critical support”
  - If the contract/subcontracts/agreements performance will involve Covered Defense Information (CDI)
- You Also Must Flow Down Subcontractor Representation and Reporting Obligations:
  - Subcontractor system compliance or request for exception to NIST SP 800-171
  - Subcontractor requirements for reporting and preservation of data re an actual or suspected cyber incident

But Wait …

- **New Guidance** – Sept. 21, 2017 Memorandum by the DoD Director of Defense Procurement and Acquisition Policy.
  - To document implementation of NIST SP 800-171 security requirements companies need:
    - A System Security Plan (SSP) in place
    - Any associated plans of action
  - Compliance completion requirement shifted to the requiring activities

New Guidance

"The only requirement for this year is to lay out what your plan is. And that could be a very simple plan, and we could help you with that plan. We can give you a template for that plan, and then just report your compliance to it."

- **Hon. Ellen Lord**, Defense Under Secretary for Acquisition, Technology & Logistics

(Testimony to Senate Armed Services Committee, Dec. 7, 2017)

New Guidance – New Questions

- Procurements after December 31, 2017:
  - Baseline requirements (SSP & POAMs) may be sufficient for contract award
  - The requiring activity may determine that full compliance with NIST SP 800-171, or something other than full, is necessary
    - Note: Under DFARS Supply Chain Risk clause, 252.239-7018, DoD may exclude an offeror if it determines that the offeror, or any proposed subcontractor, poses a supply chain risk. **DoD does not have to disclose information on the exclusion and it is not subject to review in a protest at GAO or in any Federal Court.**

New Guidance – New Questions

- Procurements after December 31, 2017 (Cont'd):
  - Per the Guidance, for some awards a requiring activity may consider the extent of an offeror's implementation of NIST SP 800-171 security requirements in its risk assessment or as a separate technical evaluation factor
    - *See, e.g., IPKeys Technologies*, LLC B-414890.2 (Oct. 4, 2017): Denying a protest where the awardee's cybersecurity framework exceeded minimum requirements and was considered superior to the protestor. Protestor's argument that the cybersecurity framework will eventually be mandatory was deemed speculative.
  - Guidance creates some level of ambiguity now
    - What to say, and when to say, something about your level of compliance
    - Seek to address questions on this as early as possible in the procurement cycle

New Guidance – New Questions

- NIST issues draft NIST SP 800-171A
  - Draft out for comment until January 15, 2018
  - Companion to NIST SP 800-171 to aid contractor's development of assessment plans and the conduct of "efficient, effective, and cost-effective assessments of the security requirements in NIST Special Publication 800-171"
  - How does it work?
    - Flexible and customizable for self-assessment or independent third party or government assessment of contractor's SSP
      - Chapter 2: Some guidance to interpret CUI requirements
      - Chapter 3: Assessment Procedures for the 14 Families of CUI security requirements in NIST SP 800-171
      - Appendices A (references), B (assessment methods), C (mapping tables)
    - Information gathering and not itself "security-producing activity"
    - Replaces "information system" with "system"

New Guidance – New Questions

- Are Requiring Activities and their personnel prepared?
- What is the pace of implementation for the SSP and POAMs?
- If all you have is an SSP and POAM, what do you need to do in a procurement?
- How does the new guidance affect stovepiping among larger contractors?
- How does the new guidance affect flow down requirements?

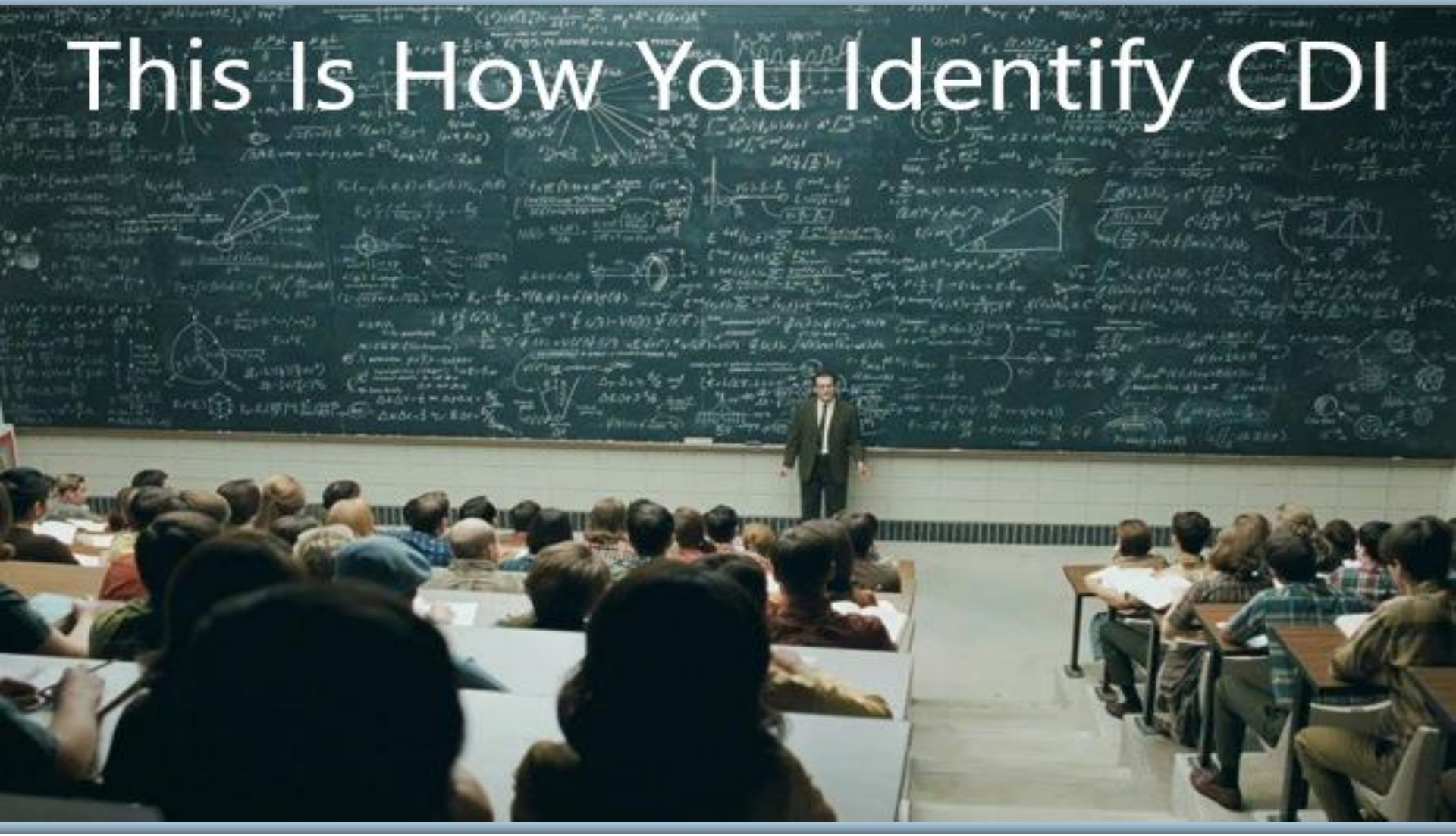
Challenges in Implementation

- For Solicitations/Contracts/Subcontracts
  - Identification of “covered defense information”, “information systems”, “subcontracts”
  - Assurance of compliance by Original Equipment Manufacturers and the rest of the supply chain
  - Investigation and Reporting
  - Preservation
  - Compliance with Other Laws
  - Protection of Data

Example: CDI Open-Ended Definition

- **Covered Defense Information:**
  - "**unclassified controlled technical information** or **other information, as described in the Controlled Unclassified Information (CUI) Registry** at [archives.gov], that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is:
    - 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
    - **Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract**"

Example: Open-Ended Definition



Challenges in Implementation

- Compliance/Noncompliance Risks and Costs
  - Present Responsibility
    - E.g., Adequate systems and controls in place
  - Protests
    - E.g.,
      - Evaluation
      - Compliance/Noncompliance
  - Claims
    - E.g.,
      - Incidents
      - Changes
  - Actual and Implied Certifications
    - Fraud Rules and Criminal Statutes

Example: False Claims Act

- Civil False Claims Act (CFCA)
  - Imposes liability where a "person" "knowingly" submits, or causes to another to submit,
    - A "false claim", "false record or statement" to the Government
    - For the purposes of obtaining payment, Government action or inaction
  - Damages
    - Assesses damages on each false "claim"
    - Damages ***per*** "claim" increased -- minimum of $10,957 to a maximum of $21,916
    - PLUS Treble Damages
  - Risk: ***Implied*** false certification theory under *Universal Health Services, Inc. v. US ex. rel. Escobar* (S.Ct. 2016)
    - Even if you have not signed a "certification"

“I Didn’t Know” Is Not An Option

Next Steps You Should Consider

- Establish your cyber security compliance team
- Determine your requirements for compliance
- Identify the data you need to protect
- Assess your current level of system compliance
- Work on your next steps, including:
  - SSP and POAM for cyber compliance
  - Cyber response plan
  - Procurements
    - Provisions in the solicitation, or the lack thereof
    - Subcontracting / teaming requirements
    - Award and administration
- Comment on Draft NIST SP 800-171A?

Possible Government Next Steps

- Additional tools to facilitate contractor compliance
- Further Guidance on DFARS Compliance – particularly for the Cloud
- “Auditing” of contractor systems and controls
- Make the DFARS cyber clause requirement applicable to the FAR

Some Key Resources

- DFARS 252.204-7012 – (https://www.law.cornell.edu/cfr/text/48/252.204-7012)
- NIST SP 800-171 – (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf)
- Guidance Memorandum (https://www.acq.osd.mil/dpap/policy/policyvault/USA003939-17-DPAP.pdf)
- PGI 204.73--Safeguarding Covered Defense Information and Cyber Incident Reporting https://www.Acq.Osd.Mil/dpap/dars/pgi/pgi_htm/current/PGI204_73.Htm
- NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information* https://csrc.Nist.Gov/CSRC/media/publications/sp/800-171a/draft/sp800-171a-draft.Pdf - **Comments due January 15, 2018**
- NIST Manufacturing Extension Partnership (MEP) Handbook 162, Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

Questions?

Susan Warshaw Ebner

Susan Warshaw Ebner is a Shareholder at Fortney & Scott, LLC. Her practice concentrates on advising and representing small and other than small businesses, non-profit and consortium clients on a broad spectrum of Federal, state and local government contract matters, including bid protests, contract procurement and administration issues, supply chain risk, cyber security, claims, audits, investigations, formal and informal dispute resolution, compliance programs, other transactions, technology investment agreements, grants, cooperative agreements. She has represented clients in courts and forums, including the U.S. Court of Federal Claims, Government Accountability Office, Boards of Contract Appeals, U.S. District and Appellate Courts, and state courts.

She is the Section Secretary of the ABA Public Contract Law Section (ABA PCLS), Co-Chair of the ABA PCLS Procurement Division, and Co-Chair, NDIA Cyber Division Legal Committee. She chaired the ABA PCLS Acquisition Reform and Emerging Issues Committee and its Task Force on Counterfeit Parts. Susan previously served as President of the Boards of Contract Appeals Bar Association, Inc., President of Women In Defense, A National Security Organization, and on the Board of Directors of the National Defense Industrial Association and the ABA PCLS Council. She is Martindale-Hubbell AV Preeminent Peer Review Rated. She can be reached at sebner@fortneyscott.com or (202) 286-4888.

Rolando R. Sanchez

Rolando R. Sanchez is a government contracts, white collar and compliance solo attorney practicing out of Washington, D.C. His current clients include companies seeking assistance with government contract and breach of contract issues. He began his career as a litigator in the U.S. Marine Corps and, after active service, represented companies in high stakes complex litigation. Part of his practice focuses on helping clients avoid litigation. He has been a thought leader in the area of cybersecurity, and has published articles, given presentations, and been interviewed by news outlets concerning developments in cybersecurity. Rolando has been an active member of NDIA's Cyber Division since its inception, where he was the chair of its legislative committee, which provided comments to various proposed legislation and contract rules. He is the current chair of the legal committee within the Cyber Division, which seeks to discuss developing cyber laws/rules with NDIA membership. Rolando is a graduate of the University of Pennsylvania Law School. He can be reached at rolando@sanchezpllc.com, (703) 835-0711.