CURRENT DEVELOPMENTS IN THE IMPLEMENTATION OF DEFENSE CYBER SECURITY RULES

A DISCUSSION OF COMPLIANCE AND ENFORCEMENT TRENDS FOR GOVERNMENT CONTRACTORS AND SUBCONTRACTORS

JUNE 6, 2019

IN CONJUNCTION WITH THE
ASSOCIATION OF CORPORATE COUNSEL
NATIONAL CAPITAL REGION

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Kelley Drye

Discussion Areas

I. Level Set – Brief Background on Legal Duties under DoD DFARS Cyber clause

II. Transition from Regulatory Implementation to Enforcement

III. Key Recommendations/Take Aways

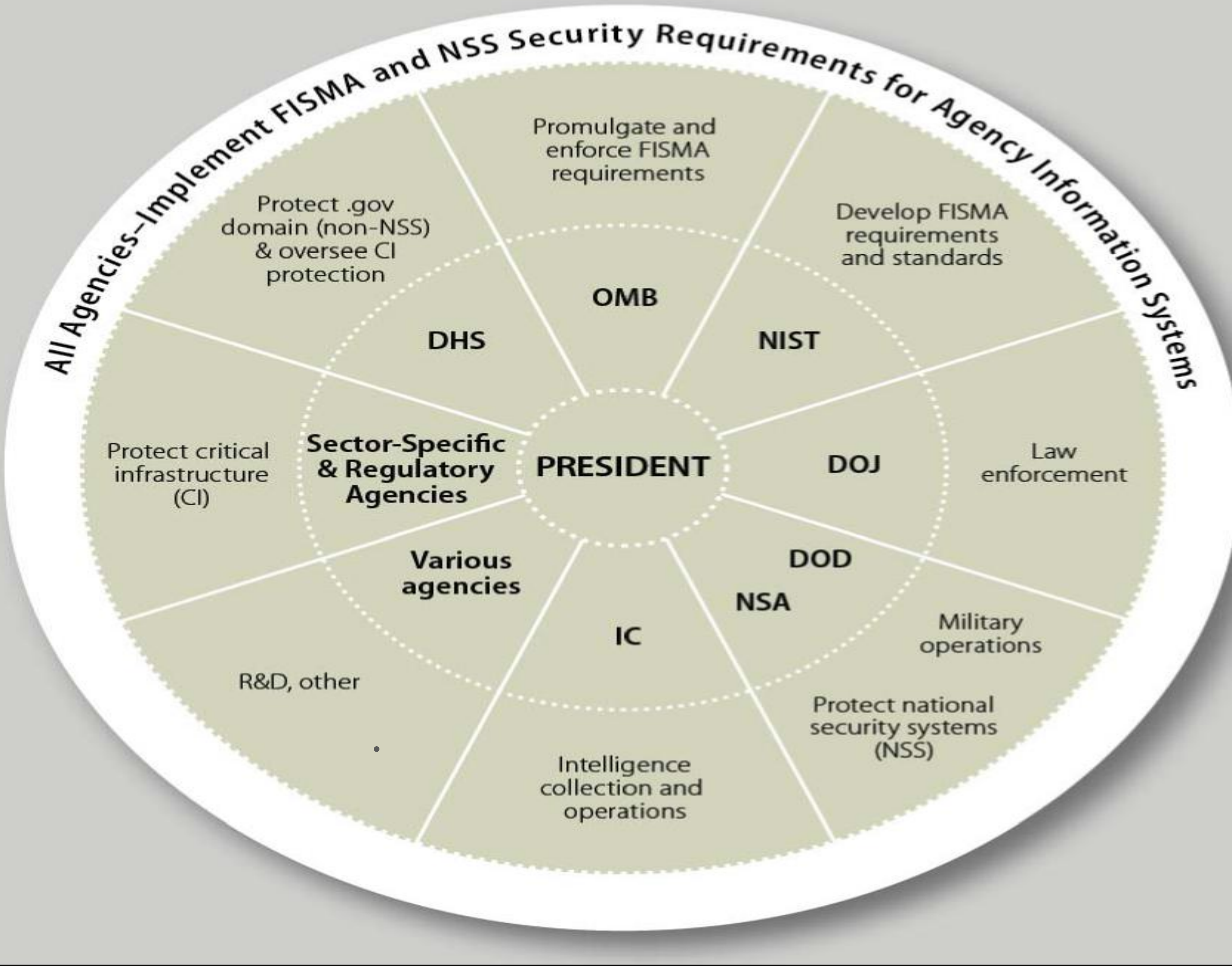
I.

BACKGROUND AND BASIC REQUIREMENTS OF DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

Kelley Drye

Brief History of Cyber Regulations

- Historically, main focus of the Department of Defense and the Intelligence Communities was protecting sensitive information through industrial security programs covering classified information (Secret, Top Secret).
- Legislative and Regulatory focus was on Federal agency information systems (FISMA) or sector specific rules (Critical Infrastructure, Healthcare, privacy).
- Principal focus was agency responsibilities.


All Agencies–Implement FISMA and NSS Security Requirements for Agency Information Systems
PRESIDENT
OMB
Promulgate and enforce FISMA requirements
NIST
Develop FISMA requirements and standards
DOJ
Law enforcement
DOD
NSA
Military operations
Protect national security systems (NSS)
IC
Intelligence collection and operations
Various agencies
R&D, other
Sector-Specific & Regulatory Agencies
Protect critical infrastructure (CI)
DHS
Protect .gov domain (non-NSS) & oversee CI protection

Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019

- **Cyber Activities Directed Against the Department of Defense**

  - Computer systems around the world, including those owned by the U.S. Government, continued to be targeted by China-based intrusions through 2018. These and past intrusions focus on accessing networks and extracting information. China uses its cyber capabilities to not only support intelligence collection against U.S. diplomatic, economic, academic, and defense industrial base (DIB) sectors, but also to exfiltrate sensitive information from the DIB to gain military advantage. The information targeted can benefit China's defense high-technology industries, support China's military modernization, provide the CCP insights into U.S. leadership perspectives, and enable diplomatic negotiations, such as those supporting OBOR. Additionally, targeted information could enable PLA cyber forces to build an operational picture of U.S. defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis. The accesses and skills required for these intrusions are similar to those necessary to conduct cyber operations in an attempt to deter, delay, disrupt, and degrade DoD operations prior to or during a conflict. In aggregate, these cyber-enabled campaigns threaten to erode U.S. military advantages and imperil the infrastructure and prosperity on which those advantages rely.

Headlines

The New York Times

June 8, 2018 "*Chinese Hackers Steal Unclassified Data from Navy Contractor*"

The Washington Post

June 23, 2018 *"Cyberattack on USIS may have hit even more government agencies."*

THE WALL STREET JOURNAL.

December 2018 *"Chinese hackers stole undersea warfare data from US Navy contractor"*

Evolution of DFARS Safeguarding Rules

- November 2013: DOD adopts NIST Standard Publication (SP) 800-53 for safeguarding Unclassified Controlled Technical Information (UCTI).
- August 2015: DoD issues first interim rule applying NIST SP 800-171 to contractors, now applies to “Covered Defense Information” (“CDI”).
- December 2015: DoD issues second interim rule allowing two year-phase in of the NIST security requirements.
- October 2016: DoD issues final rule requiring implementation “as soon as practical, but no later than December 31, 2017.”

Legal Duties of contractors and subcontractors under DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Legal Duties regarding adequate security:

- Provide adequate security on all covered contractor information systems.
  - Implement minimum security requirements - NIST SP 800-171.
  - Submit requests to vary to the Contracting Officer for consideration by CIO.
  - Require and ensure cloud service provider meets FedRAMP standards and complies with clause.
  - Apply additional information systems security measures when the Contractor reasonably determines they may be required.

Legal Duties of contractors and subcontractors under DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Legal Duties regarding cyber incident reporting:

- Rapidly Report Cyber incidents to DoD at https://dibnet.dod.mil (within 72 hours of discovery).
- Conduct review for evidence of compromise of covered defense information.
- Isolate Malicious software and submit to DoD Cyber Crime Center (DC3).
- Preserve and Protect media for at least 90 days.
- Provide DoD with access to information or equipment if necessary for forensic analysis.

Legal Duties of contractors and subcontractors under DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Legal Duties regarding subcontract flow downs:

- Include clause in “subcontracts, or similar contractual instruments,” for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items.
- Determine if the information required for subcontractor performance retains its identity as covered defense information.
- Require subcontractors to notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from NIST SP 800-171
- Provide the incident report number

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls

Certification Requirement

“By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”

What is CDI?

“Covered defense information” means 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.

What categories of information must be safeguarded? CDI.

- CDI that resides or transits through a contractor’s information systems.
- CDI includes controlled technical information with military or space applications including things such as:
  - Engineering drawings
  - Research and engineering data
  - Technical standards
  - Specifications (weapons systems specs)
  - Technical manuals
  - Export controlled information (both ITAR and EAR)

  Restrictive markings should be consulted to determine whether safeguarding is required.

What categories of information must be safeguarded? CDI includes CUI.

- CUI associated with government contracts that reside or transmit on contractor information systems must also be safeguarded.
- Examples include:
  - Critical Infrastructure
  - Financial information (Central Contractor Registration)
  - Law Enforcement
  - Nuclear
  - Personal Information
  - Proprietary Business Information

Markings to Look for: Technical Data

CDI includes newly generated technical documents delivered to the U.S. Government that include a contractor or other third party-imposed intellectual property marking.   (See DFARS 252.227-7013 - Rights in Technical Data--Noncommercial Items).

Technical Data Legend Example

LIMITED RIGHTS

Contract No. ______________________________

Contractor Name ______________________________

Contractor Address ______________________________

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(3) of the Rights in Technical Data--Noncommercial Items clause contained in the above identified contract. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such data must promptly notify the above named Contractor

(End of legend)

Markings to Look for: Export Controls

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

Markings to Look For: DoD Distribution Statements

DISTRIBUTION *STATEMENT* B. Distribution authorized to U.S. Government agencies (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION *STATEMENT* C. Distribution authorized to U.S. Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION *STATEMENT* D. Distribution authorized to Department of Defense and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

Markings to Look for: NNPI

NOFORN: THIS DOCUMENT IS SUBJECT TO SPECIAL EXPORT CONTROLS, AND EACH TRANSMITTAL TO FOREIGN GOVERNMENTS OR FOREIGN NATIONALS MAYBE MADE ONLY WITH THE APPROVAL OF NAVAL SEA SYSTEMS COMMAND.

II.

CURRENT AND FUTURE IMPLEMENTATION AND ENFORCEMENT TRENDS

Cybersecurity Maturity Model Certification (CMMC)

- Moving beyond NIST 800-171
- DoD is working with Johns Hopkins Applied Physics Lab (APL) and Carnegie Mellon Software Engineering Institute (SEI) along with Industry Partners such as the Defense Industrial Base (DIB) Sector Coordinating Council (DIB SCC), AIA and others to combine various cybersecurity standards such as, (NIST 171 & 53, ISO 27001 & 32, AIA NAS9933) and others into one unified standard for cybersecurity.
- CMMC will have basic cybersecurity basic hygiene to very robust cybersecurity requirements to create the maturity model. The CMMC will reflect the level of requirement from a level 1 to level 5. The CMMC must be semi-automated and more importantly cost effective enough at level 1 that Small Businesses can achieve minimum certification. The level of requirements for CMMC levels will be in RFP sections L & M, and will be a “go no go decision”.

Cybersecurity Maturity Model Certification (CMMC)

- The Department will be turning over the CMMC to a nonprofit as the 3rd party to train and certify firms that will become the certifiers and auditors for the CMMC. Each member company of the DoD Supply Chain will be required to obtain certification much like ISO 9000 or Capability Maturity Model Integration (CMMI).
- The 3rd party standard will be a neutral party, so that it can be agile enough to work alongside the DoD Supply Chain to be reactive and preventative as new emerging cyber threats evolve.
- The CMMC would be the center for education and training for cybersecurity. The CMMC will be the tool that 3rd party cybersecurity certifications that will provide audit capability, true metrics and more risk mitigation tools for the entire supply chain.

On the horizon: Cybersecurity Maturity Model Certification (CMMC) Implementation

- The level of technical requirements for CMMC levels will be in RFP sections L & M, and will be a "go no go decision".
- Long term - the CMMC will be addressed in a DFARS case covering DFARS 252.204.7012.
- The Department is staring listening sessions with industry in July – Aug 2019. The expected release date is Jan 2020 and will be in RFI's by June 2020.
- Both (Acting) Secretary Shanahan and Under Secretary Lord have made statements about this effort in the recent months. (noted below)
- https://www.fifthdomain.com/digital-show-dailies/air-force-association/2018/09/19/shanahan-cyber-security-will-become-fourth-critical-measurement-for-industry/
- https://www.fifthdomain.com/dod/2019/03/26/pentagon-hopes-to-have-new-cybersecurity-standards-for-contractors-in-2020/

DoD Memos & Guidance

- Sept 2018 – Enhanced cyber controls for Navy programs
- Nov 2018 – Reviewing SSPs/POAMs during acquisition & supply chain security
- Dec 2018 – Strengthened contract requirements for cyber
- Jan 2019 – Cyber oversight as part of contractor’s purchasing system review
- Feb 2019 – Strategically implementing cyber contract clauses
- Feb 2019 – DMCA Contractor Purchasing System Review Guidebook draft

ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

- ASD Kevin Fahey issued a December 17, 2018 memo SUBJECT: Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base.
- Memo “strongly encourage[s] DoD program managers and requiring activities to incorporate…sample requirements language, as appropriate, when risk to their programs and technologies warrant it.”
- Included suggested SOW language — Requesting a System Security Plan (SSP) and Any Associated Plans of Action (POA).
- Potentially included in Contract Data Requirements List as a deliverable (CDRLs)
- Restrict unnecessary sharing and/or flow down of covered defense information associated with the execution and performance of this contract based on a 'need-to-know' to execute and perform contract.

ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

Statement of Work (SOW) Paragraph x,y,z:

x.y.1. The Contractor shall, upon request, provide to the government, a system security plan (or extract thereof) and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012, and in accordance with NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" in effect at the time the solicitation is issued or as authorized by the contracting officer, to describe the contractor's unclassified information system(s)/network(s) where covered defense information associated with the execution and performance of this contract is processed, is stored, or transmits. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

x.y.2. The Contractor shall, upon request, provide the government with access to the system security plan(s) (or extracts thereof) and any associated plans of action for each of the Contractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), and the subcontractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit covered defense information associated with the execution and performance of this contract. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301.3000

USD Ellen Lord issued January 21, 2019 Memo SUBJECT: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review

- Asked Defense Contract Management Agency (DCMA) to validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012. Specifically, DCMA will leverage its review of a contractor's purchasing system in accordance with DFARS Clause 252.244-7001, Contractor Purchasing System Administration, in order to:

- Review Contractor procedures to ensure contractual DoD requirements for marking and distribution statements on DoD CUI flow down appropriately to their Tier 1 Level Suppliers.

- Review Contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301.3000

USD Ellen Lord issued Feb. 5 Memo SUBJECT: Strategically Implementing Cybersecurity Contract Clauses.

- Described the individual contract approach regarding SSPs and POAs as “inefficient for both Industry and Government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information for contracts containing DFARS clause 252.204-7012.
- Directs DCMA to develop a proposed path ahead using its administration authority under Federal Acquisition Regulation Part 42 and 43 and DFARS 242.302 to modify contracts that are administered by DCMA.
- Contemplates bilateral contract modifications that do not result in a change to any contract price, obligated amount, or fee arrangement.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301.3000

- Tasks DCMA to assess strategies to:
  - Obtain and assess SSPs and POAs strategically (not contract-by-contract)
  - Propose a methodology to determine industry cybersecurity readiness, and a level of confidence in the readiness assessment, at the corporate, business sector (division) or facility level; and
  - Propose how to communicate (document and share) that cybersecurity readiness and confidence level to the DoD Components.
  - Apply similar approach to non-DCMA administered contracts

Revised CPSR Guidebook

- Still in draft – interested stakeholders submitting comments to DCMA
- New requirements for prime contractors, including
  - Prime contractor must have procedures to assure Tier 1 Level Supplier compliance with DFARS Clause 252.204-7012 and NIST SP 800-171
  - Prime must validate that the subcontractor has a Covered Contractor Information System (CCIS) that can receive and protect CUI
  - Prime to demonstrate how it is managing and documenting subcontractors' request for variances

Implementation: Certification and False Claims Act (*qui tam*) Exposure

- *Markus v. Aerojet RocketDyne Holdings, Inc. et al*
  - Relator Brian Markus, formerly Aerojet's senior director of cybersecurity, alleges that his former employer misrepresented its compliance with cybersecurity requirements to DoD officials relating to the award of at least six contracts between 2014 and 2016.
  - Recently survived a Rule 12(b)(6) motion to dismiss the FCA allegations in the complaint.
  - DOJ <u>declined</u> to intervene.

Implementation (cont.)

- Audits
  - DoD Inspector General
  - Program audits
  - Post-incident

- Bid Protests
  - *Jordan and Howard Technologies, Inc.* (May 24, 2018)
  - *IPKeys Technologies LLC* (Oct 4, 2017)

III.

KEY RECOMMENDATIONS AND TAKEAWAYS

- Look out for revisions to NIST 800-171, DFARS 252.204-7012 and new FAR rule
- Look for Contract unique clauses beyond DFARS
- Cyber as a source selection factor (CMMC score)
- More bid protests, False Claims Act actions
- Cyber as a foundation in acquisition, not a 4th pillar
- Be familiar with the nature of controls to implement (understand each functional area and assign roles and responsibilities)
- Retain records of training and awareness efforts, audits, etc.
- Prepare for incident responses

QUESTIONS

Thank you!

DAVID HICKEY
Partner
Kelley Drye & Warren LLP
dhickey@kelleydrye.com

KATHERINE ARRINGTON
Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber
Department of Defense
katherine.e.arrington.civ@mail.mil

KRISTIN GRIMES
Corporate Counsel
Leidos
kristin.m.grimes@leidos.com

KEVIN JOYCE
Forum Co-Chair
ACC NCR
kpj2043@gmail.com

Illustrative controls to implement to become DFARS Cyber compliant

ACCESS CONTROL

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- Employ the principle of least privilege, including for specific security functions and privileged accounts.
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Kelley Drye

Illustrative controls to implement to become DFARS Cyber compliant

ACCESS CONTROL

- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
- Monitor and control remote access sessions.
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- Authorize wireless access prior to allowing such connections.
- Limit use of portable storage devices on external systems.

Illustrative controls to implement to become DFARS Cyber compliant

AWARENESS AND TRAINING

- Managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- Train personnel to carry out their assigned information security-related duties and responsibilities.
- Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Illustrative controls to implement to become DFARS Cyber compliant

AUDIT AND ACCOUNTABILITY

- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
- Review and update logged events.
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Illustrative controls to implement to become DFARS compliant

CONFIGURATION MANAGEMENT

- Establish and enforce security configuration settings for information technology products employed in organizational systems.
- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- Track, review, approve or disapprove, and log changes to organizational systems.

Illustrative controls to implement to become DFARS Cyber compliant

IDENTIFICATION AND AUTHENTICATION

- Identify system users, processes acting on behalf of users, and devices.
- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Enforce a minimum password complexity and change of characters when new passwords are created.
- Prohibit password reuse for a specified number of generations.
- Store and transmit only cryptographically-protected passwords.

Illustrative controls to implement to become DFARS Cyber compliant

INCIDENT RESPONSE

- Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
- Test the organizational incident response capability.

Kelley Drye

Illustrative controls to implement to become DFARS Cyber compliant

MAINTENANCE

- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
- Supervise the maintenance activities of maintenance personnel without required access authorization.

Kelley Drye

Illustrative controls to implement to become DFARS Cyber compliant

MEDIA PROTECTION

- Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- Limit access to CUI on system media to authorized users.
- Sanitize or destroy system media containing CUI before disposal or release for reuse.
- Mark media with necessary CUI markings and distribution limitations.

Illustrative controls to implement to become DFARS Cyber compliant

MEDIA PROTECTION

- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- Control the use of removable media on system components.
- Prohibit the use of portable storage devices when such devices have no identifiable owner.
- Protect the confidentiality of backup CUI at storage locations.

Illustrative controls to implement to become DFARS Cyber compliant

PERSONNEL SECURITY

- Screen individuals prior to authorizing access to organizational systems containing CUI.
- Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Illustrative controls to implement to become DFARS Cyber compliant

PHYSICAL PROTECTION

- Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- Protect and monitor the physical facility and support infrastructure for organizational systems.
- Escort visitors and monitor visitor activity.
- Control and manage physical access devices.
- Enforce safeguarding measures for CUI at alternate work sites.

Illustrative controls to implement to become DFARS Cyber compliant

RISK ASSESSMENT

- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
- Remediate vulnerabilities in accordance with risk assessments.

Illustrative controls to implement to become DFARS Cyber compliant

SECURITY ASSESSMENT

- Periodically assess the security controls in organizational systems to determine if effective.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- Develop, document, and periodically update system security plans (SSPs).

Illustrative controls to implement to become DFARS Cyber compliant

SYSTEM AND COMMUNICATIONS PROTECTION

- Monitor, control, and protect communications at the external boundaries and key internal boundaries of organizational systems.
- Separate user functionality from system management functionality.
- Prevent unauthorized and unintended information transfer via shared system resources.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Illustrative controls to implement to become DFARS Cyber compliant

SYSTEM AND COMMUNICATIONS PROTECTION

- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- Employ FIPS-validated cryptography when used to protect confidentiality of CUI.
- Protect the confidentiality of CUI at rest.

Illustrative controls to implement to become DFARS Cyber compliant

SYSTEM AND INFORMATION INTEGRITY

- Identify, report, and correct system flaws in a timely manner.
- Provide protection from malicious code at designated locations within organizational systems.
- Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
- Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Kelley Drye