INSIDER THREAT ASSESSMENT & CYBERSECURITY

Jonathan A. DeMella
Lisa M. Marchese

Government Contracts Practice Group

Anchorage. Bellevue. Los Angeles. New York. Portland.
San Francisco. Seattle. Shanghai. Washington, D.C. | **dwt.com**

OVERVIEW

Introduction

Trends. . .evolving threats

Security & Reporting Requirements for Contractors

Cybersecurity Update

INTRODUCTION

DATA BREACHES IN THE UNITED STATES
Recent Trends

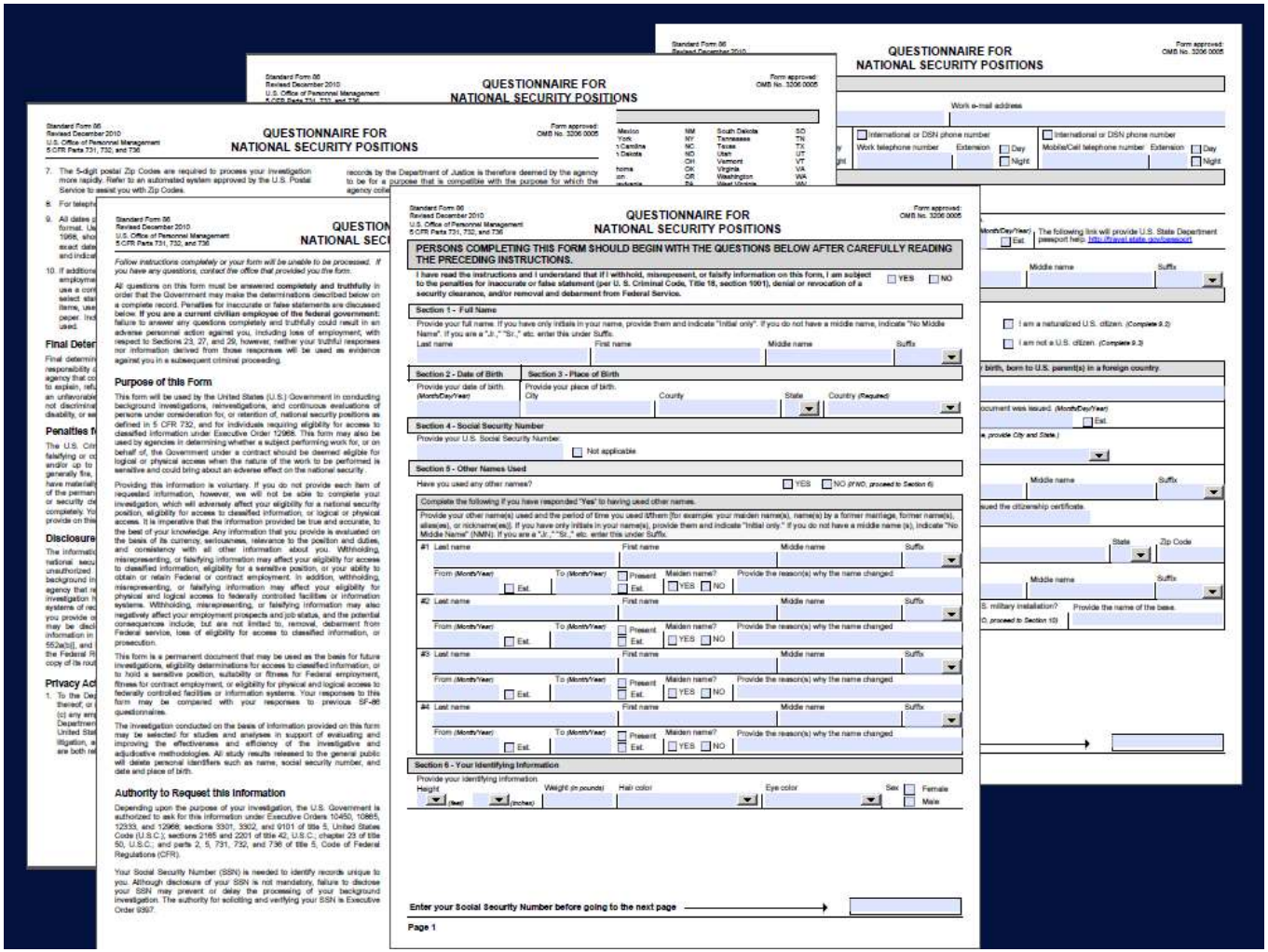
- Russian hackers, hundreds of thousands of websites, 1 billion individuals, August 5, 2014
- Anthem, Indianapolis, Indiana, 80 million individuals, February 5, 2015;
- JP Morgan Chase, New York, New York, 76 million individuals, August 28, 2014;
- The Home Depot, Atlanta, Georgia, 56 million individuals, September 2, 2014;
- Ashley Madison (owned by Canadian Avid Life Media), Toronto, Ontario, Canada, 37 million individuals (many allegedly in the United States), July 19, 2015;
- Office of Personnel Management, Washington D.C., 21.5 million individuals, June 4, 2015;
- Experian, Cost Mesa, California, 15 million individuals, October 1, 2015;
- Premera BlueCross, Mountlake Terrace, Washington, 11 million individuals, March 17, 2015;
- Excellus Blue Cross Blue Shield, Syracuse, New York, 10,000,000 individuals, September 10, 2015;
- Scottrade, St. Louis, Missouri, 4.6 million individuals, October 1, 2015;
- UCLA Health System, Los Angeles, California, 4.5 million individuals, July 17, 2015;
- Community Health Systems, Franklin, Tennessee, 4.5 million individuals, August 18, 2014;
- Medical Informatics Engineering, Fort Wayne, Indiana, 3.9 million individuals, May 26, 2015;
- Texas Health and Human Services, Houston, Texas, 2 million individuals, November 25, 2015.
- Two state-sponsored hackers in Russia believed to have broken into the Democratic National Committee servers in 2015 and 2016

THE “PEARL HARBOR” CYBER ATTACK

OPM DATA BREACH REVISITED

- June 2015 - OPM announces that it had been target of data breach affecting records of as many as 4 million federal employees
- July 2015 – number of affected people/stolen records estimated at 21.5 million and includes past, present employees and retirees
- Information targeted included personal information such as SSNs, DOBs; home addresses
- Compromised data included 5.6 million fingerprints
- Later determined that hack included detailed security clearance related background information
- Hackers believed to have been targeting files of federal employees who had applied for security clearances.
  - Form SF - 86

FORM SF - 86


Standard Form 86
Revised December 2010
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736
QUESTIONNAIRE FOR
NATIONAL SECURITY POSITIONS
Form approved:
OMB No. 3206-0005
Purpose of this Form
Authority to Request this Information
PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.
Section 1 - Full Name
Section 2 - Date of Birth
Section 3 - Place of Birth
Section 4 - Social Security Number
Section 5 - Other Names Used
Section 6 - Your Identifying Information
Enter your Social Security Number before going to the next page
Page 1

OPM Security Debacle
Catalyst for Sweeping Regulatory Changes

- Hackers suspected to be from China
- Hackers believed to have moved through government databases undetected for more than a year
- After gaining initial access, hackers were able to work their way through four additional “segments” of OPM systems
- Data breach only detected when OPM began to upgrade its equipment and systems
- OPM received multiple warnings of vulnerabilities to its information systems and security programs prior to data breach discovery – but took no action

OVERVIEW
Baseline Security & Reporting Requirements

- NISPOM Conforming Change 2
  - November 30, 2016 – Contractors to implement Insider Threat Program
- DFARS 252.204-7012
  - December 31, 2017 – Contractors to implement NIST SP 800-171. However, encourages that compliance be achieved "as soon as practical."
- Current audit data indicates that typical defense contractor is only about 60% compliant with federal cybersecurity requirements
- Lead time for contractor evaluation & implementation estimated at between 6 to 9 months

INSIDER THREAT PROGRAM

- **DSS defines "Insider Threat" as follows:**

Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DOD's ability to accomplish its mission. These acts include, but are not limited to, espionage, unauthorized disclosure of information, and any other activity resulting in the loss or degradation of departmental resources or capabilities.

- **FBI**

According to FBI, statistics, insider threat represents over 70% of cybersecurity threats.

GAO June 2015 Report to Congress
DoD Insider Threat Program

- *According to U.S. intelligence-community leaders, unauthorized disclosures of classified information by individuals with authorized access to DOD information and systems have resulted in **grave damage** to national security and potentially placed the lives of military service members at risk, highlighting the threat insiders can pose to government organizations. Disclosures by an Army service member in 2010 and a National Security Agency contractor in 2013 are among the largest known leaks of classified information in U.S. history, according to DOD and U.S. intelligence-community leaders.*

GAO June 2015 Report to Congress

Insiders with access to DOD information and systems may be able to conduct far more malicious activity-wittingly or unwittingly-than outsiders, with potentially devastating consequences for DOD. DOD's April 2015 cyber strategy stressed the importance of mitigating insider threats, stating that DOD's work to mitigate these threats extends beyond technological solutions and includes personnel, reliability, leadership, and accountability matters.

OVERVIEW
NISPOM Conforming Change 2

- Federal Contractors holding facility clearances subject to several new requirements

1. Mandatory Insider Threat Program (“ITP”)
2. New Cyber Incident Reporting Requirements
3. New NISPOM Program Components
4. New Standard for Issuance of National Interest Determinations (NIDs)

MANDATORY INSIDER THREAT PROGRAM

- Cleared contractors must have a written ITP plan no later than November 30, 2016.
  - Designation of ITP Senior Official (NISPOM 1-202)
    - ITPSO can be same person who serves as FSO
  - ITP training program for ITP Personnel and Cleared Personnel (NISPOM 3-103)
    - ITP personnel training more rigorous than other cleared personnel
    - Cleared personnel must go through training before access to classified information can be given and annually thereafter
  - Self-Inspection of Contractor Insider Threat Program (NISPOM 1.207b)
    - Completed and certified to DSS annually

INSIDER THREAT REPORTING REQUIREMENTS
Cybersecurity

- Change 2 adds new NISPOM requirements for reporting of “cyber incidents” on classified networks for CDCs.
  - Change 2 revisions consistent with FAR & DFAR cyber revisions
- “Cyber incidents” – *”actions taken thorough the use of computer networks that result in an actual or potentially adverse effect on an [Information System] or the information residing therein.”*
- CDCs must report cyber incidents on a “classified covered information system to DOD. Report must include 1) methods used; 2) sample of any malicious software used; 3) summary of potentially compromised information. (NISPOM 1-401)
- DoD has access to equipment and information of CDC that DoD determines is “necessary to conduct forensic analysis” beyond the analysis of a cyber incident conducted by CDC ((NISPOM 1-402)

NEW NISPOM COMPONENTS

- ***Adverse Information*** – any information adversely reflecting upon integrity or character of a cleared employee that suggests ability to safeguard classified information may be impaired, or that access to such information may not be in interest of national security, or that individual constitutes an insider threat.

- ***Cybersecurity*** – prevention of damage to, protection of and restoration of computers, electronic communications systems, electronic communication services, wire communication and electronic communication including information contained therein to ensure its availability, integrity, authentication, confidentiality and non-repudiation.

- ***Insider*** – cleared contractor personnel with authorized access to any government or contractor resource, including personnel facilities, information, equipment, networks and systems.

- ***Insider Threat*** – the likelihood, risk or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

NATIONAL INTEREST DETERMINATIONS

- New standard for government issuance of NID
- NISPOM 2-303c(2) – Government Contracting Activity is to determine whether release of "proscribed information" to a foreign-owned or controlled contractor operating under a Special Security Agreement "is consistent with the national security interests of the United States."
- "Proscribed information" includes Top Secret, COMSEC information, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys, Restricted Data ("RD"), Special Access Program ("SAP") information or Sensitive Compartmented Information ("SCI")

CHANGE 2
Implementation Strategies & Best Practices

- Establish an Insider Threat Program Committee
- Establish a Coordinated Cybersecurity Compliance & Insider Threat Program
- Establish process for reviewing and using available DSS and industry organization resources
    - DSS Industrial Security Letter (2016-02)
    - DSS Self-Inspection Handbook for NISP Contractors
    - National Classification Management Society publications

NIST SP 800-171 IMPLEMENTATION
NON-COMPLIANCE RISKS

- Contractor failure to timely implement DFAR & FAR mandated NIST SP 800-171 protocols by December 31, 2017 carries significant risks:
  - Breach of Contract clauses in prime and/or subcontracts
  - Liquidated damages for non-compliance
  - Termination for Default
  - False Claims Act exposure
  - Whistleblower (Qui Tam actions)
  - Mandatory disclosure to ACO when cyber requirements not met
    - Contractors must now give DoD chief information officer *"list of security requirements that the contractor is not implementing at the time of award"* within 30 days. DFARS 252.204.702
  - Suspension & Debarment for failure to make mandatory disclosure and/or perform with cyber requirements in place

DFARS 252.239-7010
Requirements for Safeguarding Information

- Contractors must have *"adequate security on all covered contractor information systems."* DFARS 252.204-7012 (b)
- Cloud computing service providers must meet security requirements set forth in DFARS 252.204-7012 (a)
- "Covered contractor information systems" is an unclassified system operated by Contractor that stores or transmits *covered defense information (CDI).*
- Definition of CDI has been the subject of considerable discussion before final rulemaking

CYBER REQUIREMENTS
Department of Defense Contracts

- "Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
- Broad Definition of "Covered Contractor Information System"
  - means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

COVERED DEFENSE INFORMATION

- Broad definition
  - Includes unclassified controlled technical information or other information (e.g. identified in CUI Registry) requiring safeguarding and/or dissemination controls
    - Marked or identified in contract as CDI
    - Collected, developed, received, transmitted, used or stored by or on behalf of contractor in support of performance of contract
- Shared obligation
  - Government has obligation to mark and identify CDI
  - Contractor has obligation to recognize and protect CDI (can't rely solely on government customer to identify CDI)

CYBERSECURITY UPDATE
Department of Defense Contracts

- *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 Governmentwide 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. Covered Defense Information includes information described in the Controlled Unclassified Information ("CUI") Registry
- Now excludes COTS items (per final rule issued October 20, 2016)

CYBERSECURITY UPDATE
DoD Contracts - CUI Registry

- Registry is online repository for information, guidance, policy and requirements on handling CUI
- Defines CUI as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies
- Executive Order 13556 "Controlled Unclassified Information" establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance.
- The heads of Executive branch departments and agencies are required to ensure implementation of the CUI program within their respective department or agency.

CYBERSECURITY UPDATE
DoD Contracts - CUI Registry

- Some Categories of CUI: CTI, Critical Infrastructure, Emergency Management, Export Control, Financial, Geodetic Information, IS Vulnerability Information, Intelligence, Nuclear, Patent, Privacy, Procurement and Acquisition, Proprietary Business Information, SAFETY Act, Statistical
- "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
  - 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.

FAR 52.204-21(b)(1)
Federal Contract Information

- FAR requires Contractors to protect information systems that process, store or transmit “Federal contract information” (“FCI”)
- FCI is defined broadly to include any information used in the performance of a contract that originated from or will be provided to the Government
- Contractor systems must meet 15 standards (includes 6 of the 14 security control families of NIST SP 800-171)

CYBERSECURITY UPDATE
FAR 52.204-21

- FAR 52.204-21, Basic Safeguarding of Contractor Information Systems
- Issued May 16, 2016 (effective date June 15, 2016)
- Adds FAR Subpart 4.19
- Applies to all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items, when a contractor's information system may contain Federal contract information

CYBERSECURITY UPDATE
FAR 52.204-21– Important Definitions

- “Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
- “Federal contract information” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
- “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

NIST SP 800-171
Overview

- Focus is on protecting CUI (inclusive of CDI)
- Over 100 security requirements
  - 30 are “basic” requirements
    - Developed from FIPS 200 (*“high level and fundamental security requirements information and information systems”*)
  - 79 are “derived” requirements
    - Developed from NIST SP 800-53 security controls

CYBERSECURITY UPDATE
DoD Contracts – NIST SP 800-171

- Purpose is to provide federal agencies recommended requirements for protecting confidentiality of CUI
- Applies to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components
- Specific requirements for nonfederal systems are designed to maintain a consistent level of protection
  - Basic security requirements derived from FIPS Publication 200, which provides high level and fundamental security requirements for federal information systems
  - Derived security requirements are from NIST SP 800-53, which set forth security controls supplementing the basic requirements

CYBERSECURITY UPDATE
DoD Contracts – NIST SP 800-171 / FIPS 200

4 SECURITY CONTROL SELECTION

Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.[5] The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve *adequate security*[6] is a multifaceted, risk-based activity involving management and operational personnel within the organization. **Security categorization** of federal information and information systems, as required by **FIPS Publication 199**, is the first step in the risk management process.[7] Subsequent to the security categorization process, organizations must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in this standard. The selected set of security controls must include one of three, appropriately tailored[8] security control baselines from **NIST Special Publication 800-53** that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- Security categorization in FIPS 199 divided among three types of potential impacts upon loss of confidentiality, integrity, or availability:
  - Low: limited adverse impact
  - Moderate: serious adverse impact
  - High: catastrophic adverse impact

NIST SP 800-171
14 Families of Security Requirements

- Defense contractors must comply with the requirements in each of the 14 families
- Contractors under the FAR must safeguard FCI in 6 families

1. Access Control
2. Awareness & Training
3. Audit & Accountability
4. Configuration Management
5. Identification & Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System & Comm. Protection
14. System & Info Integrity

CYBERSECURITY UPDATE
DoD Contracts – Assessing Compliance

- Review and apply clauses in contract
  - Clauses may supplement or supersede NIST or FIPS requirements
- Apply FIPS 199 criteria to determine the minimum standards that apply
- Map and identify security controls
  - NIST SP 800-171, Appendix D provides mapping tables of CUI requirements to the relevant security controls, including in SP 800-53 and other guidance

CYBERSECURITY UPDATE
Department of Defense Contracts - Reporting

- Reporting Requirement: Upon identification of “cyber incident”
  - Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein
  - Note that “cyber incident” not subject to uniform definition outside of Department of Defense

CYBERSECURITY UPDATE
Department of Defense Contracts - Reporting

- Upon identification of “cyber incident” contractor shall:
  - Conduct review for evidence of compromise of covered defense information
  - Analyze covered contractor information systems that were part of the cyber incident
  - Rapidly report (*i.e.*, within 72 hours of discovery) cyber incidents to DOD at http://dibnet.dod.mil
  - Preserve and protect images of all known affected information systems for at least 90 days from submission of report
  - Upon request, contractor shall provide DoD with access to additional information and systems to conduct forensic analysis

CYBERSECURITY UPDATE
DoD Contracts – http://dibnet.dod.mil

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

CYBERSECURITY UPDATE
Department of Defense Contracts – Flowdown

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), 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, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

CYBERSECURITY UPDATE
FAR 52.204-21, Minimum Security Controls

- Contractor must apply basic safeguarding requirements, which include, at a minimum, the following 15 security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(iii) Verify and control/limit connections to and use of external information systems.
(iv) Control information posted or processed on publicly accessible information systems.
(v) Identify information system users, processes acting on behalf of users, or devices.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(xii) Identify, report, and correct information and information system flaws in a timely manner.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
(xiv) Update malicious code protection mechanisms when new releases are available.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

CYBERSECURITY UPDATE
FAR 52.204-21

- 15 requirements do not refer to NIST SP 800-53 or NIST SP 800-71
- However, warns that: "This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556"
- Flowdown: "The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system."

CYBERSECURITY UPDATE
FAR 52.204-21, Conclusions

- Requirements “reflective of actions a prudent business person would employ”
- Intent is that scope and applicability of rule be “very broad, because this rule requires only the most basic level of safeguarding”
- Rule is “just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems”
- Specific enumerated controls do not refer to NIST SP 800-53 or NIST SP 800-71
- Lack of uniformity among agencies regarding rules, requirements
- Burden of compliance continues to shift to contractor
- Increased risk associated with noncompliance, data breach/loss

CYBERSECURITY UPDATE
NARA Amendments - CUI

- National Archives and Record Administration issued final rule amending its regulations on CUI (September 14, 2016)
- Final rule seeks to establish consistent practices and procedures for safeguarding, disseminating, controlling, destroying, and marking CUI
- Applies to executive agencies, but also indirectly to contractors and other information sharing partners “through incorporation into agreements”
  - This includes contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information sharing agreements or arrangements
- Defines CUI and reinforces importance of CUI Registry as exclusive means of designating CUI throughout the executive branch

CYBERSECURITY UPDATE
NARA Amendments – Implications for Contractors

- Contractors can expect to see a FAR Subpart and Clause that imposes safeguarding requirements for CUI outside of DoD contracts
- Likely that FAR will include reporting requirements for cyber incidents outside of DoD contracts
- Hopefully FAR will improve uniformity across agencies through references to established standards and controls (e.g., NIST, FIPS standards)
- Implementation period for FAR clause remains unclear

CYBERSECURITY UPDATE
Clarifications from DoD Final Rule (Oct. 20, 2016)

- Contractors are not required to implement any security requirement if an authorized representative of the DoD Chief Information Officer (CIO) has adjudicated the contractor's request to vary from NIST SP 800-171 and indicated the security requirement to be nonapplicable or to have an alternative, but equally effective, security measure
- Clarify that subcontractor flowdown is only necessary when covered defense information is necessary for performance of the subcontract, and that the contractor may consult with the contracting officer, if necessary, when uncertain if the clause should flow down
- Clarify that the prime contract shall require its subcontractors to notify the prime contractor (or the next higher-tier subcontractor) when submitting requests to vary from a NIST SP 800-171 security requirement to the contracting officer

CYBERSECURITY UPDATE
Concerns from DoD Final Rule (Oct. 20, 2016)

- "Covered Defense Information" (now aligned with definition of CUI set forth by NARA) is too broad
- Not sufficient protection for contractors forced to share information with DoD contractors tasked with processing cyber incident report.
  - Contractor may sue third party contractor, but that is insufficient in practice for protection of stolen, proprietary information
- Lack of clarity regarding standard of security cloud providers must offer
- Failure to address concerns regarding breaches of personally identifiable information revealed in incident reports

CYBERSECURITY UPDATE
Concerns from DoD Final Rule (Oct. 20, 2016)

- Failure to address concerns of small businesses

Comment: The SBA Office of Advocacy commented that the cost of compliance with the rule will be a **significant barrier to small businesses engaging in the Federal acquisition process**, adding that many small businesses will be forced to purchase services and additional software from outside and third-party in order to provide "adequate safeguards" for covered defense information and to adequately assess and evaluate their information systems and security controls.

Response: While it is understood that implementing the minimum security controls outlined in the DFARs clause may increase costs, protection of unclassified DoD information is deemed necessary**. The cost to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than these initial/ongoing investments**. The value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small). NIST SP 800-171 was carefully crafted to use performance-based requirements and eliminate unnecessary specificity and include only those security requirements necessary to provide adequate protections for the impact level of CUI (*e.g.,* covered defense information).

COMPLIANCE
RECOMMENDED BEST PRACTICES

- FORM A COMPLIANCE GROUP/TEAM
- INVENTORY OF SYSTEMS & DATA
  - Data focused approach
- OUTLINE A COMPLIANCE SCHEDULE WITH MILESTONES
- CREATE A NIST COMPLIANCE MATRIX
- ESTABLISH REGULAR INTERVALS FOR SYSTEM REVIEW AND UPDATES

CONCLUSION

Jonathan A. DeMella, Partner
Davis Wright Tremaine LLP

Jonathandemella@ dwt.com

206.757.8338

Lisa M. Marchese, Partner
Davis Wright Tremaine LLP

lisamarchese@dwt.com

206.757.8335