July 15, 2016

Industry Perspectives on Active and Expected Regulatory Actions

Alan Chvotkin
Executive Vice President and Counsel, Professional Services Council
chvotkin@pscouncil.org

Trey Hodgkins
Senior Vice-President, IT Alliance for Public Sector – ITAPS
thodgkins@itic.org

Roger Waldron
President, the Coalition for Government Procurement
rwaldron@thecgp.org

Robert S. Metzger
Head of Washington Office, Rogers Joseph O'Donnell, P.C.
rmetzger@rjo.com

Introduction

- Focus will be on new federal requirements that require contractors to safeguard federal information against cyber threats
  - The 'Network Penetration' DFARS – "Covered Defense Information"
  - The 'Basic Safeguarding' FAR – "Federal Contract Information"
  - The forthcoming "CUI Rule" – "Controlled Unclassified Information"
  - The future "General FAR" Rule to safeguard CUI
- Also will discuss safeguards: NIST SP 800-171

Chronology of Cyber/Supply Chain Initiatives

March 3, 2010	Advanced Notice of Proposed Rulemaking: "Basic Safeguarding of Contractor Information Systems"
November 4, 2010	Executive Order 13556: "Controlled Unclassified Information"
August 24, 2012	Proposed Rule, "Basic Safeguarding of Contractor Information Systems"
February 2013	Executive Order 13636: "Improving Critical Infrastructure Cybersecurity"
November 18, 2013	Interim Rule: DFARS Supply Chain Risk (Sec. 806 NDAA FY 2011)
November 18, 2013	**Final Rule: "Safeguarding Unclassified Controlled Technical Information"**
February 12, 2014	Framework for Improving Critical Infrastructure Cybersecurity
May 6, 2014	Final Rule: "Detection and Avoidance of Counterfeit Electronic Parts"
May 8, 2015	NARA Proposed Rule: "Controlled Unclassified Information"
June 19, 2015	**NIST SP 800-171: "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (Final)**
August 11, 2015	OMB draft Guidance: "Improving Cybersecurity Protections in Federal Acquisitions"
August 26, 2015	**Interim Rule: DFARS "Network Penetration Reporting and Contracting for Cloud Services"**
September 21, 2015	Proposed Rule: Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation (deletes "**embedded software**" from definition)
October 8, 2015	**DoD Class Deviation – Multifactor authentication (local/network access) – 9 mos.**
October 30, 2015	Final Rule: "Requirements **Relating** to Supply Chain Risk" (Sec. 806 NDAA FY 2011)
October 30, 2015	OMB Memorandum: "Cybersecurity Strategy and Implementation Plan" (CSIP)
November 2015	President Obama signs NDAA FY 2016 (includes cyber risk assessment)
December 18, 2015	Cybersecurity Information Sharing Act (CISA) signed into law
December 30, 2015	**Amended Interim Rule: "Network Penetration …" (defers cyber obligation to 12/31/2017)**
May 16, 2016	**Final Rule, "Basic Safeguarding of Contractor Information Systems" (81 Fed. Reg. 30439)**

Introduction

What's Been Done & Is Coming

Who's Involved

Whose Information is Affected

What Information is to be Protected

What Safeguards Apply

The 3-Part Federal Initiative to Safeguard CUI

There are three elements to the federal CUI initiative:

① NIST's SP 800-171, establishing cyber safeguards expected of commercial companies and other non-federal actors who host, use or transmit CUI **Done**

② NARA's CUI Rule, establishing categories of CUI, responsibilities for designation, dissemination controls and required cyber security measures (NIST SP 800-171 for CUI on non-federal information systems) **Final Rule: Expected Soon?**

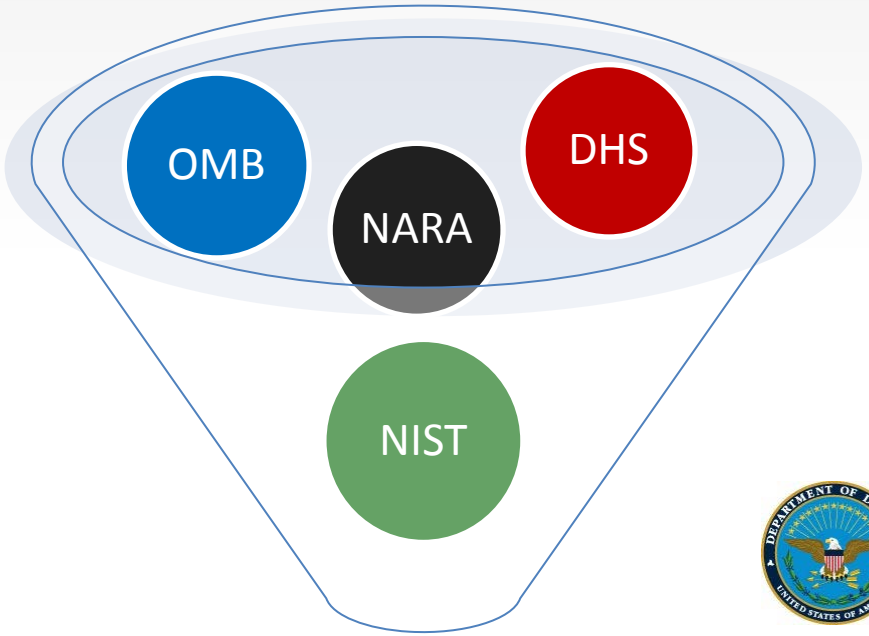
③ Acquisition Measures, effected by regulation, implemented through solicitation requirements and contract clauses, to obligate recipients to protect CUI, e.g.,

- *DoD's "Unclassified Controlled Technical Information" DFARS (Nov. 2013)* **Superseded**
- *DoD's Interim DFARS, "**Network Penetration Reporting and Contracting for Cloud Services**" (Aug. 2015, revised Dec. 2015)* – protects four categories of CUI termed "Covered Defense Information" (CDI) **Applies now to DoD contracts**
- *DoD, GSA & NASA Final FAR, "**Basic Safeguarding of Contractor Information Systems**" (May 2016)* **Effective June 15, 2016**

Expected from OMB: the final cyber "acquisition guidance"

Expected from NARA: a *General FAR Rule* to protect all forms of CUI

Federal Initiatives: Roles & Missions



ACQUISITION METHODS & CONTRACT CONTROLS - TOOLKIT

FAR & DFARS

Contractors who receive CUI will become subject to federal cyber obligations as these are imposed by regulation or contract term.

Responsibilities:

OMB: to decide on the policies to use acquisition methods and contract tools

NARA: to define and categorize the varieties of "CUI" and establish workable guidelines & mechanisms

NIST: to identify required security controls and practices for adoption

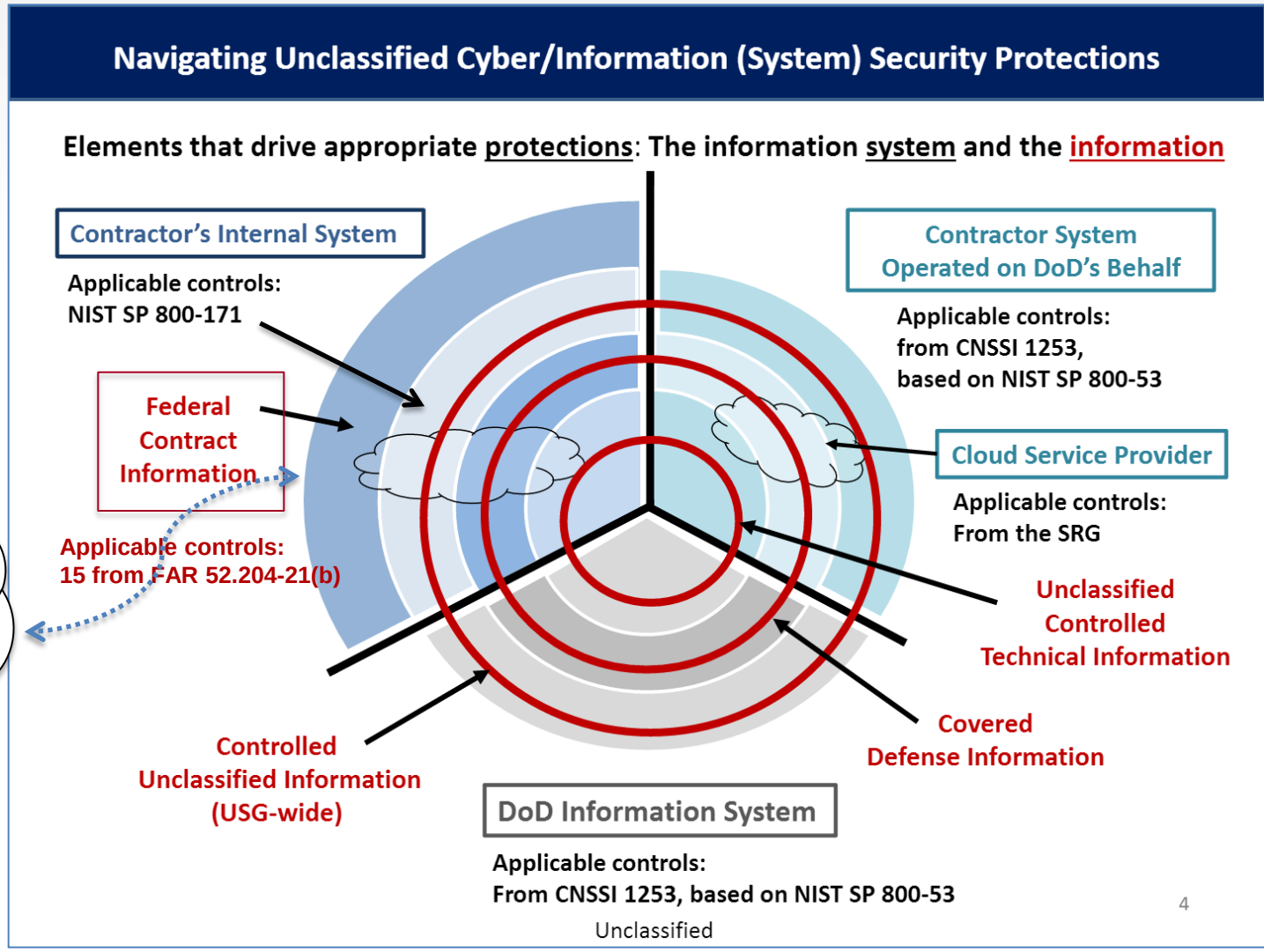
DoD: lead agency for contractually-imposed cyber requirements

DHS: to coordinate cyber incident response (US-CERT), for protection of critical infrastructure, and (new) to assist in contractor self-assessment and control implementation

Agencies: to evaluate cost/benefit, tailor, specify reporting, require monitoring, administer and oversee

Affected Information System Domains

Adapted from DoD, "Navigating Unclassified Cyber/Information Security Protections, Network Penetration Reporting and Contracting for Cloud Services," Dec. 17, 2015, available at http://www.cogr.edu/COGR/files/ccLibraryFiles/Filename/000000000292/Navigating%20Unclassified%20Information%20System%20Security%20Protections%20(slides%20for%20COGR)Thursafternoon.pdf



Categories of Controlled Unclassified Information

- NARA Proposed Rule: "Controlled Unclassified Information"), 32 CFR Part 2002, 80 Fed. Reg. 26501 (May 8, 2015)

- NARA's CUI "Registry," https://www.archives.gov/cui/registry/category-list.html, identified 23 Categories and 82 Subcategories of CUI

Who has access to CUI?

Federal contractors
State & Local governments
State & Local contractors
Tribal governments
Colleges & Universities
Interstate Organizations
NGOs
Foreign governments

Agriculture	**Controlled Technical Information**	**Critical Infrastructure (7 sub)**	**Emergency Management**	**Export Control (1 sub)**
Financial (8 sub)	**Foreign Government Information**	**Geodetic Product Information**	**Immigration (7 sub)**	**Information Systems Vulnerability**
Intelligence (5 sub)	**Law Enforcement (15 sub)**	**Legal (11 sub)**	**NATO (2 sub)**	**Nuclear (5 sub)**
Patent (3 sub)	**Privacy (8 sub)**	**Procurement & Acquisition (2 sub)**	**Proprietary Business (3 sub)**	**SAFETY Act Information**
Statistical (3 sub)	**Tax (1 sub)**	**Transportation (2 sub)**	"CUI categories and subcategories are those types of information for which ***laws, regulations, or Government-wide policies*** requires safeguarding or dissemination controls". Proposed 32 C.F.R. § 2002.2 (Definitions)	

NARA estimates that 300,000 contractors & grantees hold Controlled Unclassified Information

NIST SP 800-171: 14 "Families," 109 Controls

SP 800-171 describes 30 "basic" and 79 "derived" security requirements.
"Basic" tracks to control families in FIPS-200; "derived" reflect NIST SP 800-53 rev4.

Access Control (2/20)	Awareness & Training (2/1)	Audit & Accountability (2/7)	Configuration Management (2/7)	Identification & Authentication (2/9)
Incident Response (2/1)	Maintenance (2/4)	Media Protection (3/6)	Personnel Security (2/0)	Physical Protection (2/4)
Risk Assessment (1/2)	Security Assessment (3/0)	Systems & Comm Protection (2/14)	System & Information Integrity (3/4)	

SP 800-171 does not require submission of a Security Plan and has no mechanism for authorization, accreditation or for government review or approval. Instead, SP 800-171 relies on self-assessment and self-attestation. Cyber breaches will require reporting and federal inquiry could follow events.

CUI used to produce a product, provide a service, or perform a function, will be subject to SP 800-171.

The ‘Network Penetration’ DFARS Effective December 30, 2015

Features of the 'Network Penetration' DFARS

- Applies to "Covered Defense Information" (CDI) which is
  - **"[p]rovided to** the contractor by or on behalf of DoD in connection with the performance of the contract" or "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor **in support of** the performance of the contract" and is one of
  - [1] **Controlled Technical Information**; [2] Critical Information (Operations Security); [3] **Export controlled** information; or [4] other information that requires safeguarding pursuant to "**law, regulations, and Governmentwide policies"**. [corresponds to CUI criteria]
- "Compliance" clause (-7008) and "Safeguarding" clause (-7012) to be included "in **all solicitations and contracts**," including FAR Pt. 12; -7012 is to flow down "without alteration."
  - Compliance Clause (-7008). As revised, includes representation that contractor "will implement" requirements of SP 800-171 "not later than **December 31, 2017**."
  - Safeguarding Clause (-7012). Effective upon receipt. Obligation to provide "**adequate security**" + **reporting** requirement with 72 hours of discovery of any cyber incident. Requirement to **advise within 30 days** of contract award of -171 requirements **not met**.
- Cloud Computing. For DoD use, CSP must have "provisional authorization" per DISA's "Security Requirements Guide" (FedRAMP+) (≠ SP 800-171).

Issues and Objections

Key Issues

- Are contractors at risk for CDI not identified to them?
- How do multinational companies implement this rule?
- What assistance can be rendered by the DoD CIO's office or the CO?
- How to assure compliance with the "adequate security" obligation?
- What mechanics satisfy the objectives of SP 800-171?
- How to assure supplier compliance?
- How to affordably and practicably meet MFA obligations?
- What rules apply to CDI in the cloud?

Key Objections

- The Rule is a surprise
- The regulatory target is moving
- Acts of different federal agencies are not sufficiently coordinated
- Changing to NIST SP 800-171 will be very difficult and expensive
- Contractors can't be certain what is "covered defense information"
- Conflict with export controls
- Uncertainty as to exceptions, deviation or approval process
- Concerns about enforcement
- Small business unable to comply

Discussion

- What needs to be clarified?
- What needs to change?
- What does industry need from DoD customers?
- What might be improved in SP 800-171
- How can we assist the supply chain?
- Will the DFARS produce ‘adequate security’
- How will DoD be assured that contractors deliver “adequate security” and meet -171?

The ‘Basic Safeguarding’ FAR Effective June 15, 2016

"Federal Contract Information" (FCI)

Applies to "Federal contract information" (FCI)

- FCI defined *very broadly* as nonpublic information that is "provided for or generated for the government" **– all agencies** – under a contract to "develop or deliver a product or service to the government, but not including information provided to the public or simple transactional information. It excludes information made available by the Government to the public or "simple transactional information". FAR 52.204-21(a)
- *"Information"* also is defined broadly – to include "any communication or representation of knowledge such as facts, data, or opinions, in any medium or form". FAR 4.1901; 52.204-21(a)

Protects "information systems"

- The new FAR protects "information systems" rather than carefully defined information types. If a contractor "processes stores or transmits" any FCI, its information system becomes "covered" by the Rule and subject to minimum enumerated safeguards. FAR 4.1901; 52.204-21(a), (b)
- Where an information system hosts FCI, the rule applies to the whole system.

Applies to all acquisitions (ex. COTS)

- The "Basic Safeguarding" rule applies to "**all acquisitions**" (including commercial items other than COTS) when a contractor's information system "may contain" FCI; the FAR contract clause is to be inserted in "when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system." FAR 4.1902, 4.1903

15 safeguards derived from SP 800-171

1) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3) Verify and control/limit connections to and use of external information systems.
4) Control information posted or processed on publicly accessible information systems.
5) Identify information system users, processes acting on behalf of users, or devices.
6) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
7) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
8) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
9) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
10) 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.
11) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
12) Identify, report, and correct information and information system flaws in a timely manner.
13) Provide protection from malicious code at appropriate locations within organizational information systems.
14) Update malicious code protection mechanisms when new releases are available.
15) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Basic Safeguarding: Questions and Concerns

How will industry respond?

- The 'Network Penetration' DFARS met with strong industry resistance because of uncertainty over costs and how to comply. The 'Basic Safeguarding' Rule applies to *many* more contracting actions, contracts and contractors – and undoubtedly will surprise (and may alarm) some.
- The Rule presumes these safeguards are consistent with "prudent business practices." Even so, some companies will object to perceived "federal interference" and cyber mandates.
- It can be very difficult to assure compliance to high level standards without resort to more prescriptive (and expensive) regimes for guidance.
- No present experience to inform about costs or value of this rule.

Are there problems with the 'Basic Safeguarding' Rule?

- Yes. The Rule seeks to apply simple security propositions to highly complex subject and diverse business circumstances. There are drafting issues that will surface as more and different companies confront compliance obligations that are *now* imposed.

Is this Rule important?

- While self-described as "just one step in a series of coordinated regulatory actions being taken or planned", it reflects a government decision to use its regulatory power and acquisition authority to mandate minimum cyber defenses for *all* private companies that do government business
- Lessons learned will be relevant to the more demanding "General FAR CUI Rule" to come.
- Implications for participation in the supplier base are TBD.

Discussion

- Why is this rule needed?
- How will it affect different industry segments?
- Are there resources to assist with assessment?
- What is the cost of implementation?
- How to reconcile the 15 safeguards with other cyber defense practices?
- Is there a reporting obligation?
- How will federal agencies administer or enforce?

What's Expected

Actions Pending

- OMB's final guidance – "**Improving Cybersecurity Protections in Federal Acquisitions**"
  - Sets federal policy for application of cyber rules to contractors
  - Five elements: ❶ Adequate Security Controls [171] ❷ Cyber Incident Reporting ['Net Pen' DFARS] ❸ Information Systems Security Assessments [?] ❹ Information Security Continuous Monitoring [?] ❺ Business Due Diligence [GSA RFI, SCRM Provenance Pilot, May 9, 2016]
- NARA's Final Rule – "**Controlled Unclassified Information**" (Proposed May 2015)
  - Will designate and define the categories and subcategories of CUI
  - Expected to set the basic and derived safeguards required (and rely on SP 800-171)
  - Unsure whether agencies will cede so much authority to NARA or accept -171 as sufficient
- The "**General FAR CUI Rule**" (Proposed Rule date – unknown)
  - Goal will be consistent treatment of all forms of CUI
  - Expected to impose SP 800-171 safeguards upon all recipients of every form of CUI
  - May also include mandatory reporting
  - Expect at least 1 year for notice-and-comment rulemaking

The "General FAR Rule" will have profound effect upon the hundreds of thousands of entities that receive, transmit or host any form of Controlled Unclassified Information

About the Presenter: Bob Metzger

This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

Robert S. Metzger
Rogers Joseph O'Donnell PC
202-777-8951
Rmetzger@rjo.com

Bob heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a boutique law firm that specializes in public procurement matters. He advises leading U.S. and international companies on key public contract compliance challenges and in strategic business pursuits. Bob is recognized for work on supply chain and cyber security. On these subjects, he has published extensively and has made presentations to many academic, government, industry, legal and technical groups.

Naming him a 2016 "Federal 100" awardee, Federal Computer Week said of Bob: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Bob is a member of the Defense Science Board Cyber/Supply Chain Task Force. He also is Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Industry Council (ITIC), a prominent trade association.

Bob received his B.A. from Middlebury College and his J.D. from Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs (now "Belfer Center"), Harvard Kennedy School of Government. Bob is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on national security topics include articles in *International Security* and the *Journal of Strategic Studies*.