Strafford

Presenting a live 90-minute webinar with interactive Q&A

New Cybersecurity Requirements for DoD and Non-DoD Government Contractors: NIST SP 800-171 Compliance

TUESDAY, MAY 8, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Townsend L. Bourne, Partner, **Sheppard Mullin Richter & Hampton**, Washington, D.C.

Tina D. Reynolds, Partner, **Morrison & Foerster**, McLean, Va.

David Verhey, Partner, **Dunlap Bennett & Ludwig**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-961-8499** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

New Cybersecurity Requirements for DoD and Non-DoD Government Contractors: NIST SP 800-171

A Strafford Webinar presentation

Tina Reynolds, Morrison & Foerster LLP
treynolds@mofo.com

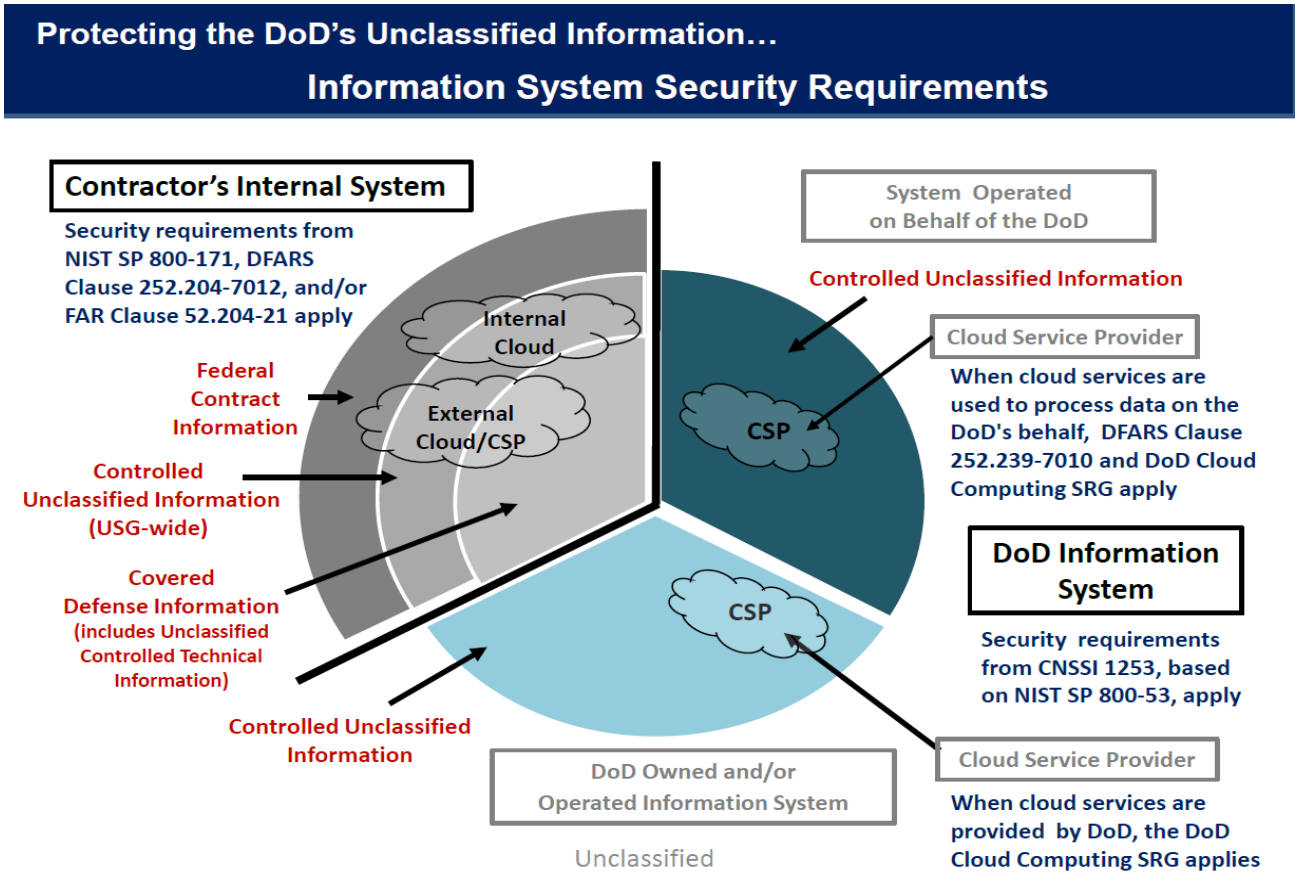
May 8, 2018

Introduction

Topics to be addressed:

- Relevant regulations and guidance
- Compliance obligations and penalties for non-compliance
  - Developing a POAM/SSP
  - Business considerations for data management
- Subcontractor cybersecurity management

Summary of USG cybersecurity systems



SheppardMullin

Cybersecurity: Government Contractor Regulations & Standards

TOWNSEND BOURNE
tbourne@sheppardmullin.com
Partner, Sheppard Mullin Richter & Hampton LLP

Controlled Unclassified Information (CUI)

- **Sensitive**, but not classified
- Approved by NARA and reflected in the **CUI Registry**
  - https://www.archives.gov/cui/registry/category-list
- New categories of CUI can be created through law, regulation, or government-wide policy; NARA can recognize "provisional categories"
- Current Categories Include:
  - Controlled Technical Information
  - Export Control information
  - Privacy information (e.g., PII and health information)
  - Procurement and Acquisition information
  - Proprietary Business Information

National Archives and Records Administration (NARA) CUI Final Rule (Nov. 14, 2016)

- Establishes framework for handling CUI
- Requires "**reasonable precautions**" to guard against disclosure of CUI (based on NIST)
- Establishes two types of CUI:
  - **CUI Basic**. The default CUI standard; sharing must be in furtherance of a lawful government purpose and not otherwise prohibited by law, amongst other requirements.
  - **CUI Specified**. The law, regulation, or government-wide policy articulates different sharing and safeguarding standards. CUI Registry should reflect these specific requirements.
- Establishes marking standards (No more FOUO or SBU)
- FAR Rule promised that will mimic NARA CUI Final Rule

NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

- Catalog of security and privacy controls for **federal information systems** (except national security systems)
  - Covers systems operated *on behalf of* an agency by a contractor
  - Over 150 Moderate Impact Controls (also includes controls for "low" and "high")
- Includes **18** security control families
- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* - Provides specific guidelines for periodically assessing security controls

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- Protects Controlled Unclassified Information (CUI) for **non-federal information systems**
- Includes "basic" and "derived" requirements
  - Basic requirements originate from FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
  - Derived requirements come from NIST SP 800-53
- NIST SP 800-171 is tailored to non-federal systems and does not include the unique federal controls in NIST SP 800-53
- Rev. 1 (Dec. 2016) added control for System Security Plan

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

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

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- NIST MEP Handbook 162, "Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements" (Nov. 20, 2017)
  - Intended for "small manufacturers"
  - Assessment questions related to NIST SP 800-171 security requirements
- Draft NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" (Nov. 28, 2017 & Feb. 20, 2018)
  - Assessment procedures for all security requirements in NIST SP 800-171
  - Mapping tables and guidance in Appendices
  - Final publication will address comments submitted March 23, 2018

FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Protects **"Federal Contract Information" (FCI)**
  - FCI is "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"
  - Excludes publicly available information or "simple transactional information, such as necessary to process payments"
- Contractor information systems that process, store, or transmit FCI are subject to **15 basic security requirements** from NIST SP 800-171
- Flow-down: All subcontracts (except for COTS) where the subcontractor may have FCI "residing in or transiting through its information system"
- No requirement for contractor to report cyber incidents

DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

- DoD contractors must provide "adequate security" for **"covered defense information" (CDI)**
  - CDI is unclassified controlled technical information, further described at http://www.archives.gov/cui/registry/category-list.html, which is marked and provided by the Government to the contractor, or otherwise generated/accessed by the contractor, for contract performance
- **"Adequate security"** means compliance with the NIST SP 800-171 standards, except:
  - May need additional controls if dictated by a risk assessment (DFARS 252.204-7012(b)(3))
  - There are separate standards for cloud computing services (*see* DFARS 252.239-7010) and for information systems operated "on behalf of" the Government (*see* NIST SP 800-53)

DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

- Deadline: No later than **December 31, 2017**
  - Implementation means a **System Security Plan** and **Plans of Action**
  - Note: May be used as an evaluation factor and in source selection
- Flow-down: All subcontracts involving CDI or "operationally critical support"
  - If using an external cloud service provider, vendor must comply with the FedRAMP Moderate baseline
- Incident Reporting: "Rapidly report" (within 72 hours of discovery)
- Cyber incident requirements:
  - Submit malicious software discovered to DoD Cyber Crime Center
  - Preserve media of affected systems for at least 90 days, and share with DoD if it conducts a damage assessment
  - Comply with DoD requests for access to additional information or equipment necessary for forensic analysis

Agency-Specific Regulations

- Contractors need to be familiar with their customer agency's policies
  - *E.g.,* VA, State Department, DHS, GSA
- Requirements may include:
  - Submitting an "IT Security Plan"
  - Accreditation and authorization
  - Providing security training to employees and possibly subcontractors
  - Maintaining procedures for detecting and reporting security incidents
- Be mindful of agency-specific reporting requirements
  - Review contracts
  - Who?
  - Time frame
  - What triggers reporting obligation?

Agency-Specific Regulations

- DHS – in the process of amending its Homeland Security Acquisition Regulation (HSAR)
  - Plan to require adequate security and privacy measures to safeguard CUI and facilitate improved incident reporting
  - New rule would establish a number of new categories of CUI, in part to address types of sensitive information not adequately protected in the present CUI framework
  - Proposed rule published and comments submitted in 2017

- GSA – plans to implement two new cyber regulations in 2018
  - Cybersecurity requirements to be implemented in GSA Statements of Work
  - Establish uniform reporting requirements for cyber incidents

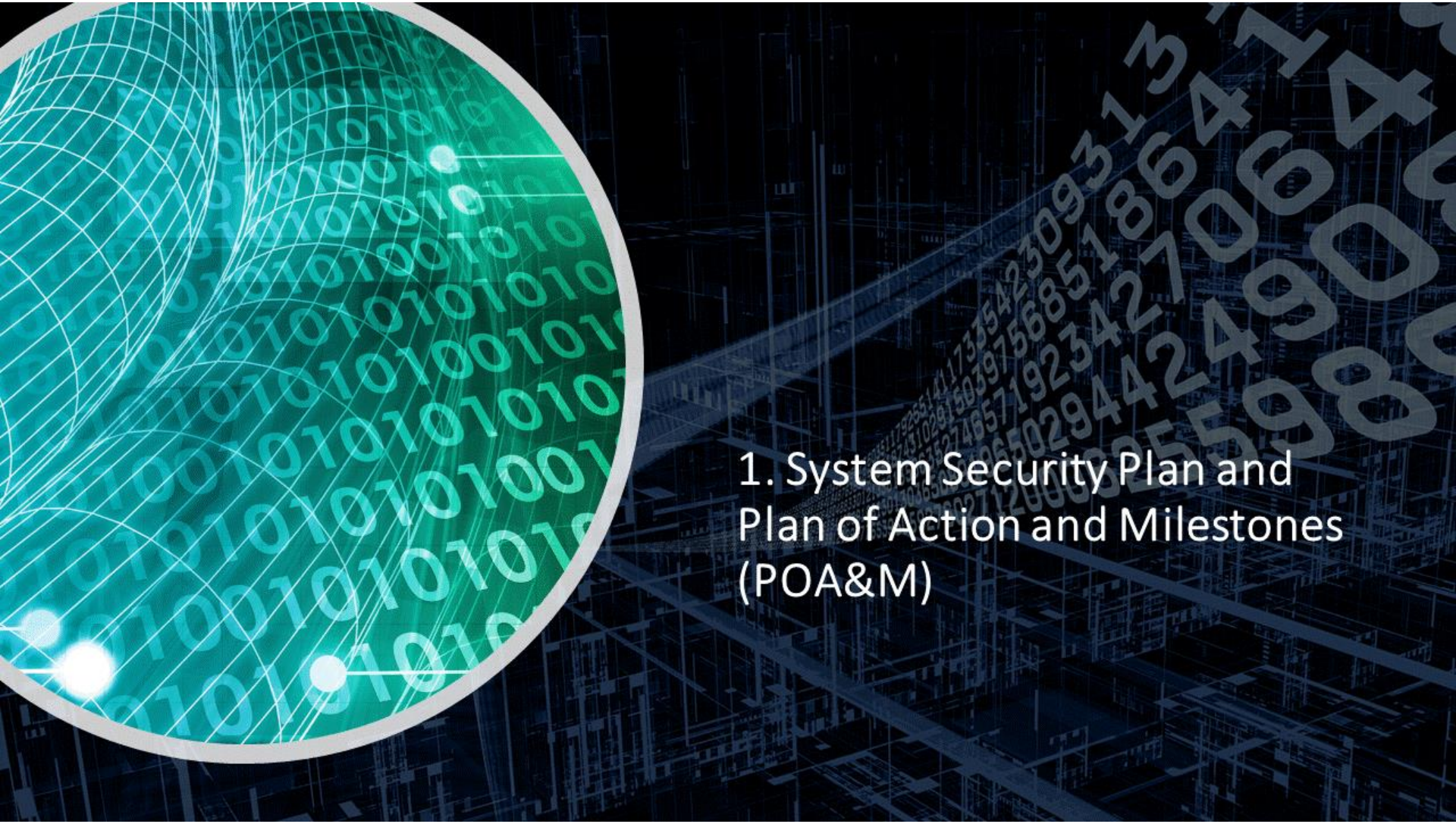
NIST 800-171/DFARS Compliance and Penalties:

Key Steps & Business Concerns

David M. Verhey, Partner
Dunlap, Bennett, & Ludwig PLLC

Three Key Points:

1. System Security Plan and Plan of Action and Milestones (POA&M)
2. Penalties
3. Business Concerns


1. System Security Plan and
Plan of Action and Milestones
(POA&M)

2. Penalties for Noncompliance


3. Business Concerns

DUNLAP BENNETT & LUDWIG

1717 Pennsylvania Ave NW #1025
Washington, DC 20006
202-731-16976
dverhey@dbllawyers.com

MORRISON FOERSTER

SUBCONTRACTOR-RELATED CYBERSECURITY CONSIDERATIONS

Subcontractor Compliance

- Ensure necessary cybersecurity requirements are communicated to subcontractors, and that they are held accountable for compliance.
  - Subcontract terms must include all necessary cybersecurity flowdowns (e.g.
  - can include indemnification provisions for breach incidents
- Most recent DoD guidance suggests prime should limit sharing of CDI and thus the need for flowdown
- Not sufficient to merely flow down applicable clauses - some level of diligence is required
  - Detailed communication with subcontractors of specific requirements of the DFARS cyber clause (or other applicable clause)
    - fully implement the requirements outlined in the clause and NIST 800-171
    - Cyber incident reporting
    - Flowdown to lower tier subs

Subcontractor Compliance

- Consider requiring that the subcontractor provide a certification and/or evidence of its NIST 800-171 compliance
    - Ensure it has developed a system security plan and plan of action and milestones to resolve any gaps.
- Investigate independently (particularly if you have reason to suspect lack of compliance)

Options where Subcontractor is Non-Compliant

- If subcontractor communicates non-compliance with NIST 800-171 or other applicable standards:
  - Terminate subcontract
  - Restructure work to prevent subcontractor access, use, generation of CDI
  - Move subcontractor to your site to perform work (or otherwise provide compliant IT systems for subcontractor use)
    - Can also put on site with government customer
  - Assist subcontractor with development of SSP/POAM
  - Request relief from government customer
- DoD is establishing Procurement Technical Assistance Centers (PTCAs) and working with industrial base to ensure that supply chain is compliant
  - Especially designed to help small and medium sized businesses
- Remembers costs of cybersecurity compliance are generally allowable.

Subcontractor Cyber Incident Reporting

- No specific clause for non-DoD agencies, but special clauses generally require flowdown
- DoD "network penetration" rule (DFARS 252.204-7012)
  - Mandatory flowdown to subcontractors if they will store, process, or generate CDI
  - Subcontractor must notify DoD (via DIBNet reporting system) and provide the incident report number to the prime contractor.
    - Prime can request more detail in its subcontract agreement, although subcontractors will resist sharing of proprietary information about system vulnerabilities

MORRISON FOERSTER

RESOURCES & MATERIALS

Resources and materials

- FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Jun 2016); https://www.ecfr.gov/cgi-bin/text-idx?SID=b4f7168959b9f6102111de9dd93c4622&mc=true&node=se48.2.52_1204_621&rgn=div8
- DFAR 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016); https://www.ecfr.gov/cgi-bin/text-idx?SID=67beab7d711b779823a65a8846deecf0&mc=true&node=se48.3.252_1204_67012&rgn=div8
- NIST Special Publication 800-171, Rev. 1 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
- NIST Framework for Improving Critical Infrastructure Cybersecurity, v. 1.1 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST Special Publication 800-53, v.5, Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Resources and materials (cont.)

- NIST MEP CYBERSECURITY Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security
- DoD's June 23, 2017 Industry Information Day charts http://dodprocurementtoolbox.com/site-pages/cybersecurity-other-resources
- DoD April 2, 2018 update to Frequently Asked Questions (FAQs) regarding DFARS Subparts 204.73 and 239.76 (covering DFARS 252.204-7012 and 252.239-7010) https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf
- Office of the Under Secretary of Defense, Memorandum: "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" (Sept. 21, 2017) http://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf
- Defense Procurement & Acquisition Policy guidance http://www.acq.osd.mil/dpap/pdi/docs/p2p%20training%20presentations/Cybersecurity%20Initiatives%20&%20Requirements.pdf


MORRISON
FOERSTER