DFARS & NIST 800-171 Data Protection Requirements

Bio

Paul Dodd
Senior Technical Fellow
Boeing Information Security Chief Strategist

Paul is responsible for the information security strategy to effectively protect Boeing's data and IT resources.

Bill Kenney
Director, Information Security
Corporate, Enterprise Services and Chief Strategy Office

Bill has responsibility for enterprise information security and strategy at Northrop Grumman Corporation.

Timothy J. Smith
Chief Architect
Rockwell Collins Enterprise Security

T.J. is responsible for enterprise security and compliance strategies and roadmaps.

Bob Deragisch
Director, Engineering Services, IT Infrastructure and eBusiness
Parker Hannifin Corporation

Bob is responsible for managing the IT technologies for engineering systems at the Aerospace Group of Parker Hannifin Corporation.

National Archive (NARA) CUI Registry

- Export Controlled Information
  - Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. Includes dual-use items.
- Controlled Technical Information (UCTI)
  - 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.
- Critical Infrastructure
  - Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
- Information System Vulnerability Information
  - Related to information that if not protected, could result in adverse effects to information systems.
- Procurement and Acquisition
  - Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
- Proprietary Business Information
  - Manufacturer - company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.

DFAR / FAR Rule - Summary

- **6/2015 NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"**
  - Introduced new security standard SP 800-171 - 109 Controls derived from SP 800-53 (Moderate)
- **08/25/15- 252.204-7012 - "Safeguarding Covered Defense Information & Cyber Reporting"**
  - Introduced "Controlled Defense Information"
- **08/25/2015 - 252.204-7008 "Compliance with safeguarding covered defense information controls."**
  - Introduced 72 hour reporting requirements for all compromises
  - Ability to utilize 3rd party contractors to investigate compromises and ability to share data related to a compromise investigation as the government sees appropriate
- **12/30/15- Second interim rule issued**
  - Amends DFARS provision to provide additional time to implement the security requirements – compliant by December 31, 2017
  - Within 30 days of contract award, notify the DoD CIO of any NIST SP 800-171 security requirements that are not implemented at the time of contract award.
- **5/16/2016 – FAR 52.204-21 Federal Contract Information (FCI) – Basic Safeguarding of Covered Contractor Information Systems**
  - Apply 15 general security controls on covered systems for basic level of "safeguarding" of federal contract information
- **8/15/2016 – NIST Publishes New Draft of SP 800-171 and requests comments**
  - Introduced Security Plan (110th control) and POA&M
- **9/14/2016 – 32 CFR Part 2002 – "Controlled Unclassified Information (CUI)"**
  - Replaced FOUO & other unclassified labels
  - Required NIST SP 800-171 controls for all types of CUI, effective Nov 14, 2016

NIST SP 800-171 - Summary

NIST SP 800-171 Requirements			
NIST 800-171 Control Family	**Required Controls**	**NIST 800-171 Control Family**	**Required Controls**
3.1 Access Control	22	3.8 Media Protection	9
3.2 Awareness and Training	3	3.9 Personnel Security	2
3.3 Audit and Accountability	9	3.10 Physical Protection	6
3.4 Configuration Management	9	3.11 Risk Assessment	3
3.5 Identification and Authentication	11	3.12 Security Assessment	4 *
3.6 Incident Response	3	3.13 Systems and Communication	16
3.7 Maintenance	6	3.14 System and Information Integrity	7
Total Controls Required (Basic and Derived)			**110**

* One Requirement added to recent Draft of NIST SP 800-171r1. Establishes the need for a System Security Plan and Plan of Action and Milestones to track compliance. Although in draft format, we expect it will be a requirement in the updated version of 800-171

Industry Partnerships

CODSIA
Council of Defense and Space Industry Associations

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

AIA
AEROSPACE INDUSTRIES ASSOCIATION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Compliance Approach

- **Enterprise-wide coordination with Legal, Contracts, Supplier management, IT and others**
- **Update Cyber Incident Response Team (CIRT) process**
- **Flow down requirements to sub-tier suppliers**
- **Assess applications and systems in the enterprise, programs, and cloud service providers**
- **Be aware of problematic areas:**
  - **Multifactor Authentication, Session Protection & Replay Resistant Authentication**
  - **FIPS Validated cryptography**

Q & A

Backup

Contact Information

Paul Dodd
Paul.Dodd@Boeing.com

Bill Kenney
Bill.Kenney@ngc.com

Timothy J. Smith
tj.smith@rockwellcollins.com

Bob Deragisch
Bderagisch@parker.com

References

- **DoD DIB CS Program:** http://dibnet.dod.mil/
- **NARA CUI Registry:** https://www.archives.gov/cui/registry/category-list.html
- **DFARS Regulation 48 CFR 252.204-7012 (CDI):** https://www.federalregister.gov/articles/2015/12/30/2015-32869/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for
- **DoD Frequently Asked Questions:** http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contracting.html
- **FAR Regulation 48 CFR 52.204-21 (FCI):** https://www.federalregister.gov/articles/2016/05/16/2016-11001/federal-acquisition-regulation-basic-safeguarding-of-contractor-information-systems
- **32 CFR Part 2002 (CUI):** https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information
- **NIST SP 800-171:** http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf