Assured Information Technology

The Key To Your Information Assurance

NIST 800-171, DFARS

RESPONSIBILITIES FOR DEFENSE SYSTEMS AND BEYOND FOR FEDERAL SYSTEMS AFTER 31 DECEMBER 2017

18 October 2017

Jason Eddy

AIT Engineering

NIST 800-171 Overview

- Purpose
  - Improve protection of Controlled Unclassified Information (CUI)
  - Improve protection of Covered Defense Information (CDI)
  - Ensure timely reporting of Cybersecurity incidents
- Scope (Digital Security)
  - Physical and Environmental Security
  - Operational Technology Security
  - Information Technology Security
  - (New Focus) Personnel Information
- How
  - Protect CUI and CDI via regulations, policy and guidance
  - Define 14 Control families and 110 individual controls
  - Focus on Confidentiality, Integrity, and Availability of information
  - Safety / Harm (Additional provision over and above traditional CIA)
- When
  - Before 31 Dec 2017 for DOD Contractors
  - After 31 Dec 2017 for other US Government Agency Contractors

DFARS CLAUSE 252.204-7012

Assured Information Technology
The Key To Your Information Assurance

- DFARS Clause 252.204-7008,7009, 7012 (Covered Defense Information, 21 October 2016) clause MUST be included in ALL contract actions with no exceptions, including, but not limited to:
  - Request for Quote (RFQ) against all GSA Schedule Contracts
  - Request For Information (RFI)
- DFARS scope covers, at a minimum, the following categories
  - Anything related to CTI
  - DFARS expands known CTI term to now include anything related to Operations Security, transportation, logistics, personnel falls within scope
  - International Traffic in Arms Regulation (ITAR)

- **Current:** DoD and Subcontractors, and those supporting Federal Executive Branches storing, processing, transmitting DoD and Federal Civilian Executive branch agencies by 31 December 2017*

- **After December 31, 2017:** Requirements for ALL federal agencies to require protection of CUI/CDI per SP 800-171 in all future contractual requirements. *FAR rule expected by December 2017***

*Service providers, including Cloud Service Providers (CSPs), credit card, financial, web, e-mail service providers, communication (satellite, cell, cable)

** National Archives and Records Administration (NARA) estimates 300k+ contractors, colleges, tribal nations, universities, NGO's and Foreign Governments will have to comply.

Why Are So Many Now In Scope?

Assured Information Technology
The Key To Your Information Assurance

- Greatest number of breaches occur due to third-party affiliates, contractors and subcontractors, not DOD
- CUI has been collected quite successfully over the last few years via numerous security breaches by Advanced Persistent Threats (APTs)
- Data gathered directly impacts our national security interests
- As a result, the US government is now fast-tracking the NIST 800-171 regulatory requirements and the DoD is citing DFARS to enforce
- The US Government now requires DoD 'Covered Contractor Information Systems' to provide 'Adequate Security'
  - DFARS defines 'Adequate Security' as: *Providing adequate security measures commensurate with consequences and probability of loss, misuse, unauthorized access, or malicious modification of information*

Examples Of CUI Personnel Data Directly Impacting National Security

Assured Information Technology
The Key To Your Information Assurance

'The loss or improper safeguarding of CUI can have a serious adverse effect on organizational operations, organizational assets, or individuals."

- Recognized that significant degradation of mission capabilities to perform contractual obligations has been significantly reduced due to numerous security breaches involving CUI and CDI Information
- OPM Data Breach of 2015
  - Security clearance background investigation information on 22 million individuals.
  - Cost taxpayers $350 Million for notification
- Anthem / Blue Cross Blue Shield (BCBS) breach
  - Provides insurance for more than 2 million US government employees and 9 million US Government contractors
- Equifax Breach, 143 Million and counting
  - Exposed credit accounts worth of $100B
  - Recent contract award from IRS to provide identity services

Timeline

Assured Information Technology
The Key To Your Information Assurance

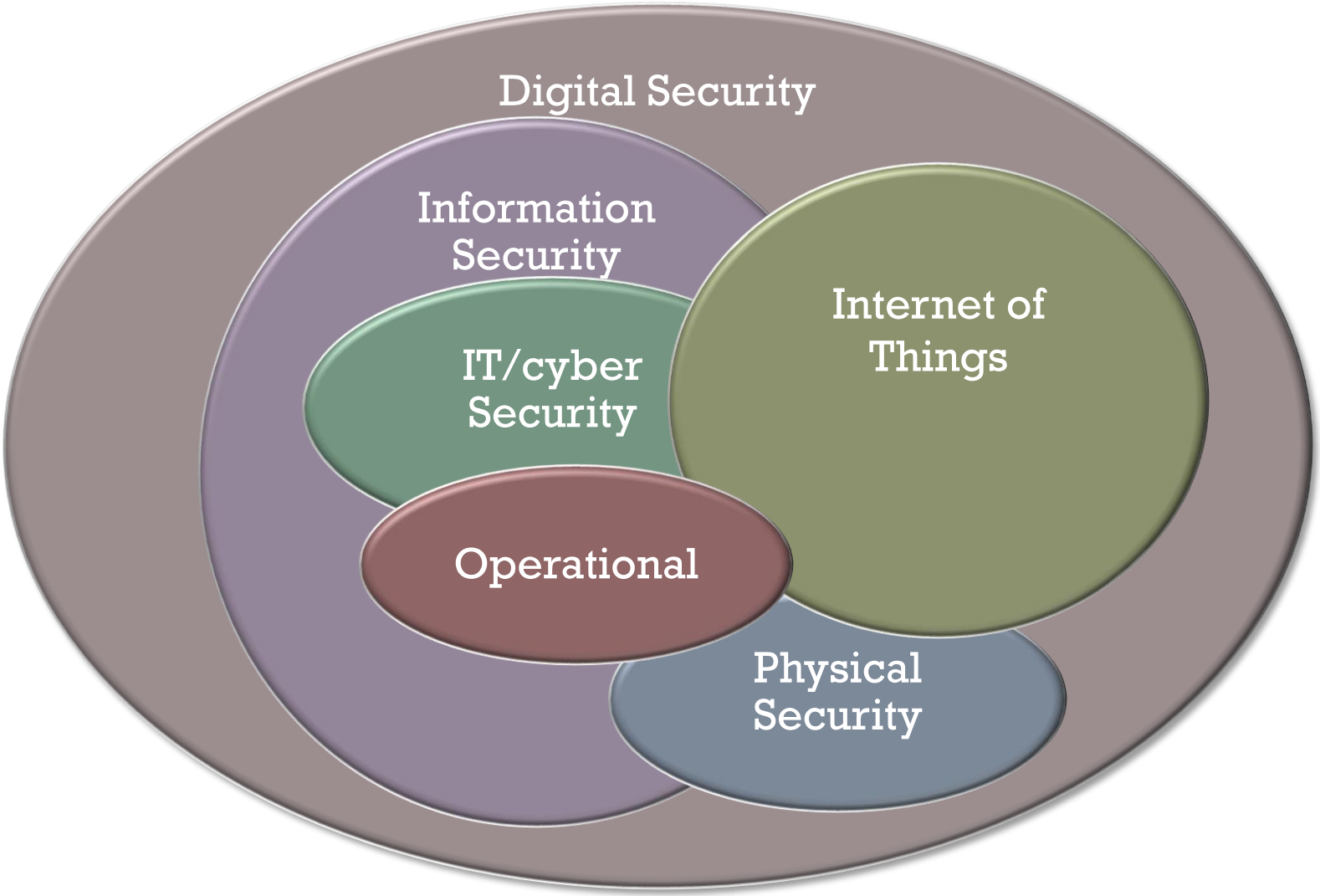
- **DIACAP**
  (May 2009 – October 2014)
- **RMF** (Strongly based on NIST 800-37 and 800-53)
  (October 2014 – Present)
- **NIST 800-171**
  (RMF still in place, but NIST 800-171 required NLT 31 December 2017 for DoD contractors and subcontractors**)
  - Self-certification is required at this time with no independent approvals
- **Penalties for Noncompliance**
  - Inability to bid on contracts
  - Contract Terminations
  - Criminal Fraud
  - Negligence Fines and Penalties

Non-DOD/Contractors CUI's Affected After 31 December 2017

- Agriculture
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Intelligence
- International Agencies and agreements with same (EU, etc.)
- Law Enforcement
- Legal
- Nuclear
- Patents
- PHI, PII
- Procurement and Acquisition
- Tax (IRS, State, local)
- Transportation
- Statistical Information not sufficiently pseudonymized.

What NIST 800-171 Addresses

Assured Information Technology
The Key To Your Information Assurance



Data Definitions

Assured Information Technology
The Key To Your Information Assurance

- **Covered Contractor Information System (CCIS)** – unclassified system owned or operated by a contractor that processes, stores, and transmits 'Covered Defense Information
- **Covered Defense Information (CDI)** – unclassified controlled technical information as defined in CUI Registry.
- **Controlled Unclassified Information (CUI)**
- **Controlled Technical Information (CTI)**. Military or space application subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, dissemination. (DoD 5230.24)
- Examples
  - Engineering data and drawings
  - Manuals
  - Technical reports / orders
  - Data sets, studies and analyses
  - Executable and software source code
  - Personnel Information
  - Financial Information

NIST 800-171 Priorities

- Category 1 items include: Devices that store, present, or process CUI or CDI data
  - File Servers
  - Email Servers
  - Backup Servers
  - SharePoint Servers
- Category 2 items include: Devices that support controlling access of CUI or CDI Data
  - Domain Controllers
  - Firewalls, routers, switches
  - Antivirus/Anti-malware servers (locally or web hosted)
  - Patching servers
  - Jump Boxes (Remote Desktop)
- Category 3 items include: Other devices not used in the storing or protection of CUI or CDI Data

**If CUI/CDI information is properly segmented from the rest of your operations, then the Federal Government will not consider your entire organization's network 'in scope.' **

14 Control Groups

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance

14 Control Groups Continued

- Media Protection
- Personnel Security
- Physical Security
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Information Integrity

Where To Begin

- Determine where CTI, CDI, and CUI is processed, stored and transmitted (Due Care)
- Perform a Gap Analysis
  - Complete NIST 800-171 Questionnaire for compliance with 14 Control Groups
    - Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
    - If using Exostar, also available and required there by major Prime Contractors
  - Focused Security Assessment addressing all NIST 800-171 controls to determine current compliance and where 'gaps' exist. (Scope exercise)
    - Business Impact Analysis (BIA)
    - Business Continuity Plan / Disaster Recovery Plan (BCP/DRP)
      - Don't overlook key vendors and subcontractors
- Evaluate business need to handle CUI (Due Diligence)
  - Stop collecting CUI if no business need and dispose appropriately (physical, electronic, encrypt)
  - Migrate required CUI data/processes and consolidate to reduce scope, improve controls, and reduce overall risk

Compliance Roadmap

Assured Information Technology
The Key To Your Information Assurance

- Accurately Identify CDI and CUI
  - Do not overlook benefit of segmenting networks and access
- Comprehensive Policies and Procedures Describing Protections
  - Training and Awareness Policy
  - Access Control Policy
    - Includes Physical and Technical
    - Must address Multi-factor authentication
  - Account Management Policy
    - Uses Least Privilege and Separation of Duties (When Possible)
  - Disaster Recovery / Business Continuity Policy
  - Continuous Monitoring Policy
  - Media Protection Policy
  - Cyber Incident Reporting Policy
    - Must utilize https://dibnet.dod.mil
    - Must report within 72 hours

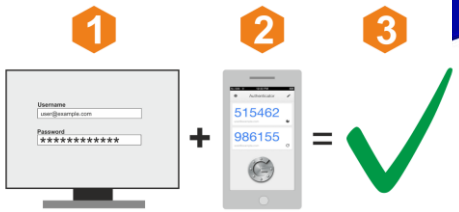
- Consider outsourcing compliance obligations by storing CDI in a FedRAMP approved cloud
  - https://www.fedramp.gov
  - https://marketplace.fedramp.gov/index.html#/products?sort=productName

Due Care And Due Diligence

- **Due Care** – care an ordinary person would normally exercise under potential or actual circumstances
  - Policies, Procedures, Standards, Guidelines, Best Practices
  - Business Continuity Plan / Disaster Recovery Plan
    - Business Impact Analysis (BIA)
  - Document roles and responsibilities
    - Map to Access Controls and attest to compliance with NIST 800-171
- **Due Diligence** – Ongoing effort to avoid harm to another party
  - Conduct technical compliance audits (PCI-DSS 3.x, SOX, GLBA, FFIEC, GDPR, Privacy Shield)
  - Periodic (Annual) Risk Assessments
  - Performance Reviews

Expected Challenges

- Multi-factor Authentication



- NIST 800-171 Appendix D interpretation concerning non-privileged accounts using multi-factor authentication. (Control 3.5.3)
  - Only Systems Administrators are required to use multi-factor authentication, regardless of location (local or remote)
  - System users only need multi-factor when accessing via VPN connection.
  - NIST 800-53 rev 4.
    - NIST 800-171 Appendix D maps to NIST 800-53 IA-2(I), IA-2(2), IA-3(3)
- Continuous Monitoring Program
  - Requires both procedural and technical solutions to monitor system
  - Free COTS or Open Source solutions may be sufficient to meet needs
    - COTS tool Splunk
      - http://www.splunk.com
      - Free for up to 500 MB/day, Considerably expensive for higher rates
      - Existing NIST Compliance Dashboards
      - Low Setup and Configuration Effort
    - Open Source Tool ELASTIK
      - http://elastik.sourceforge.net/
      - Some existing NIST Compliance Dashboards
      - Free with unlimited data processing
      - Moderate Setup and Configuration Effort

AIT OVERVIEW

Assured Information Technology
The Key To Your Information Assurance

- Veteran-owned Small Business Founded in 2011
- Located at 12001 Research Pkwy, Suite 128
- Primarily Focused on Cybersecurity and Information Technology
- Experts in Risk Management Framework (RMF)
- Subject Matter Experts in all related areas
  - Networks (Cisco, Juniper, SonicWall, etc.)
  - Databases (Oracle, SQL, Postgres, NoSQL, Cassandra, etc.)
  - Software Development (Java, C#, C++, etc.)
  - Operating Systems (Windows, Linux, Android, MAC, Apple IOS, etc.)
  - Policy (Configuration Management, Change Control, Software Dev)
  - Compliance (FISMA, Sarbanes Oxley, HIPAA, Penetration testing, etc.)
  - Virtualization (VMware, Hyper-V, Amazon Web Services, Microsoft Azure, etc.)
  - Wireless (802.11, 802.16, Cellular, Bluetooth, Microwaves, etc.)
- AIT personnel achieved over 100 Authority to Operate (ATO) with 100% Success
- Developed and fielded over 30 Cross Domain Solutions (CDS)
- DoD 8570.01-M Certified workforce with DoD, DoS, DHS, DoD contractor and commercial expertise

How AIT Can Help

Assured Information Technology
The Key To Your Information Assurance

- No-cost consultation to provide assessment framework and compliance roadmap
- Developing RMF docs and achieving Accreditation
- 'Deciphering' Requirements versus Directives with RMF, NIST 800-171, NARA, DFARS, and NIST 800-53 and 800-37
- Continuous Monitoring Setup Assistance or via Managed Services
  - Extensive Experience with Splunk configurations and monitoring
- Multi-factor authentication analysis and implementation r
- Development and sustainment of required Policies and Procedures

Reference / More Information

- AIT Engineering www.aitengineering.com
  - Jason Eddy e-mail: Jason.eddy@aitengineering.com
- Department of Homeland Security (DHS)
  - https://www.dhs.gov/enhanced-cybersecurity-services
- Department of Defense Cyber Crime Center (DC3)
  - https://www.dc3.mil
- Approved Cloud Service Providers
  - https://marketplace.fedramp.gov/index.html#/products?sort=productName
- NIST Special Pub 800 Series
  - http://csrc.nist.gov/publications/PubsSPs.html#SP 800
- DISA STIGs
  - http://iase.disa.mil/stigs/Pages/index.aspx
- PCI-DSS 3.x (Open PCI DSS Scoping Toolkit)
  - https://www.pcisecuritystandards.org