Advanced Institute for Manufacturing

NIST 800-171 Workshop

NIST 800-171 Importance for Manufacturers

- DFARS 252.204.7012 Contract Clause
  - CUI: Controlled Unclassified Information
- Compliance Deadline: 12/31/17
  - Deadline already extended from 2015
  - Plan of Action/System Security Plan may be acceptable
  - Strictness of compliance will vary based on contract
  - Vendors may “Comparison shop”
  - No auditing/certification currently in place
    - CMMC Certification coming in 2020
  - Self-assessed

NIST 800-171: A Summary

- NIST 800-171 Special Publication
  - Cross-References NIST 800-53
  - HR and IT Team involvement
  - 14 Sections, 110 Items

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

3.1 Access Control

- Key Factors:
  - How employees access CUI
  - User account login controls and permissions
  - Separation of duties/Least privilege requirements
  - User timeouts/logouts
  - Remote access/VPN controls
  - Wireless network access
  - Mobile device encryption
  - CUI on publically accessible systems

3.2 Awareness and Training

- Key Factors:
  - Proper IT/Cybersecurity policies
    - Definition of CUI as well as handling/transmission
    - Best Practices, password requirements, removable media, etc.
  - Training for all employees
    - New Employee Orientation
    - Re-training for existing employees 1-2 times per year
    - Review policies, awareness training, insider threat training

3.3 Audit and Accountability

- Key Factors:
  - Creation and retention of system audit records:
    - Server and Network logs
    - Regular review of activity
    - On-demand report generation
    - Automated alerts on security incidents
    - Controls on audit features (Restrict to administrator)

    - Software can offer ease of monitoring and report generation at a price (Money vs. Time)

3.4 Configuration Management

- Key Factors:
  - Establish inventory of system hardware and software
  - Establish and enforce security configuration settings
  - Ensure no changes are being made to systems without security impact considerations
  - Disable/Restricted unnecessary ports, functions, services
  - Employ software blacklisting/whitelisting policies

3.5 Identification and Authentication

- Key Factors:
  - User Authentication (Login credentials)
  - Multi-factor authentication
  - User account management (identifier re-use, disabling inactive credentials
  - Password management (Length/complexity requirements, temporary passwords, password re-use)

3.6 Incident Response

- Key Factors:
  - Establish formal incident response system
  - Document security/IT-related incidents
    - Managed by IT dept/Security officer
    - Information on current and resolved incidents
      - Time/person who reported, incident description, source, resolution
    - Test incident response system
      - Phishing e-mails, tabletop exercises, social engineering tests
    - Must be able to provide incident information to contractors/authorities

3.7 Maintenance

- Key Factors:
  - Regular system maintenance (Operating systems, software, etc.)
  - Control maintenance techniques (IT department)
  - Equipment sanitization for off-site maintenance
  - Scanning of maintenance tools and software
  - Supervision of unauthorized maintenance personnel

3.8 Media Protection

- Key Factors:
  - Media usage policies
    - CUI controls (prohibition, markings, encryption)
  - Sanitization/Destruction of decommissioned system media
  - Prohibition of “unknown devices”
  - Protection of backup CUI

3.9 Personnel Security

- Key Factors:
  - Screening of employees handling CUI
    - Background checks, references, prior employment
  - Protection of CUI during personnel actions
    - Transfers, terminations
      - No access for non-employees

3.10 Physical Protection

- Key Factors:
  - Physical Infrastructure Access (PCs, servers, networking equipment
  - Facility security (Building access and monitoring)
  - Supervision and tracking of visitors and guests
  - Physical device access control (Keys, keycards, fobs, codes, etc.)
  - Safeguards at alternate work sites (Remote locations, home offices, etc.)

3.11 Risk Assessment

- Key Factors:
  - Periodic assessment of risks and assets within company (including CUI)
  - Regular vulnerability scans and assessment as new vulnerabilities are discovered
  - Remediation based on assessment findings

3.12 Security Assessment

- Key Factors:
  - Regular assessment of security controls
  - Developing/Maintaining System Security Plan
  - Developing/Maintaining Plan of Action
  - Continual monitoring of security controls on ongoing basis

3.13 System and Communications Protection

- Key Factors:
  - Network architecture
  - Communications traffic (Incoming and outgoing)
  - Transmission of CUI
  - Prevention of shared resources (Cross-connection of networks)
  - Subnetting of publically accessible systems
  - Collaborative computing device controls (Webcams, conference microphones, etc)
  - Monitoring and segregation of VoIP systems
  - Control usage of mobile code (Java, JavaScript, ActiveX, macros, etc.)

3.14 System and Information Integrity

- Key Factors:
  - Reporting systems flaws in a timely fashion
  - Installation of anti-virus/anti-malware
  - Regular scanning of client and server systems
  - Updating protection software as new definitions are released
  - Generation of alerts in the event of malicious software detection.