Quick Start Strategy to Compliance
DFARS 252.204-7012

Rob Gillen
Overview

• Meet FASTLANE
• Important Updates
• Overview of NIST 800-171
• Case Studies
• 5 Items to a Quick Start Strategy to Compliance...NIST 800-171/DFARS
  1. Boundary Definition
  2. Policy and Personnel Assessment
  3. Technical Assessment
  4. System Security Plan (SSP) and Plan of Actions and Milestones (POA&M)
  5. Cloud-based Solutions
Important Updates

• NIST 800-171 Rev 1 Update Released 28 Nov 2017
• NIST 800-171A in draft
  – Assessment guide
  – Provides testing (assessment) guidance
  – Requesting industry feedback – comments due 27 Dec 2017
  – Derived from NIST 800-53A
  – Assist organizations in:
    • Developing assessment plans
    • Conducting assessments
What is NIST 800-171?

• Protection of Controlled Unclassified Information (CUI) in non-federal systems
• Executive Order 13556 – National Archives and Record Administration (NARA) as executive agent
• DoD, GSA and NASA require contractors to implement specific security measures and report non-compliance to the CIO by December 2017
• What's covered??
  – Anything related to "performance of the contract"
CUI Categories Defined by NARA

- Agriculture
- Controlled Technical Information
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Geodetic Product Information
- Immigration
- Information Systems Vulnerability Information
- Intelligence
- International Agreements
- Law Enforcement
- NATO Information
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business
- SAFETY Act Information
- Statistical
- Tax
- Transportation
NIST 800-171 Security Families

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

- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity
5 ITEMS TO A QUICK START STRATEGY TO COMPLIANCE...NIST 800-171/DFARS
• Where does my CUI reside?
• Minimize the CUI footprint within your organization
• Define what systems, processes, programs, applications, hardware, software, people, etc. fall under the scope of your NIST 800-171 compliance
• Understand dataflow to know:
  – What users and components have direct access to CUI?
  – What users and components have indirect access to CUI?
  – What users and component control access to CUI?
- Understand which IT assets fit within the boundary.
- Interconnections: indicate and label interconnections to other systems
- Make sure your boundary is consistent with hardware & software inventory
- Make sure your diagrams are consistent with boundary descriptions
Large majority of the CUI controls in 800-171 are policy based
Starting with strong organizational policies will enforce process and compliance
Supplementing current policies with new requirements provides less impact
Phase in new policies
Determine to whom and what the new policies apply
Educate all staff on new policies
Any policies requiring new technology, processes or personnel must be analyzed within the organizational strategy
#3 Technical Assessment

- Assess your current security status IAW NIST 800-171
- Conduct a gap analysis to determine non-compliance
- FIPS 140-2 encryption for CUI?
- Data-at-Rest solution?
- Multi-factor authentication?
- Audit logging, review and management?
- Incident Response?
#4 SSP and POA&M

- System Security Plan (SSP) identifies compliance with NIST 800-171 security controls
- 14 families of security controls
- Focused around confidentiality
- Based of FIPS 200
- Ensure compliance with any deficiencies identified in your gap analysis or request approval from CIO.
- Plan of Actions and Milestones (POA&M) is developed
• Compliance is a full-time commitment
• Not just documentation
• Can be implement in cloud-based solutions or on premise
• Requires a policy, procedures and tools to implement
• Automation is KEY!
Summary

Boundary Definition
Know what is included in your CUI boundary.

Policy and Personnel
Policy drives compliance and procedures for meeting the technical requirements.

Technical Assessment
Review all technical controls in place against the NIST 800-171 requirements

System Security Plan
The backbone to your system documentation.

Continuous Monitoring
Full-time commitment.
Case Studies

Nothing in this presentation is an endorsement of a particular company, technology or solution!

Names and titles of the guilty parties have been changed!
Case Study #1: Gem City Geeks

15 People IT contracting company providing out-sourcing solutions, such as website hosting, IT maintenance and network management to prime contractors. Mostly remote employees.

**Gap Analysis Findings**

- No Data at Rest (DAR) solutions
- No Multi-Factor Authentication (MFA)
- No organizational policies documented.
- No background checks conducted on employees.
- No vulnerability assessments conducted on internal assets.
- No configuration management of internal assets.
- ....................

**Solutions to Compliance**

- Deployed FIPS-compliant BitLocker for Windows 10 laptops.
- Legacy laptops were upgraded.
- YubiKey for local authentication to Windows laptops
- POA&M documented and employee handbook drafted.
- Employee handbook updated to ensure that all employees hired who worked on DoD prime contractor sites have background checks conducted
- POA&M documented and Vulnerability management policy drafted. All users will be required to bring their laptop in monthly for scanning.
- POA&M documented and a CM Program initiated. Initial policy developed and asset inventory completed.
- Many more POA&M items developed and incorporated into a Cybersecurity Strategy that requires executive buy-in
50 employee company providing mostly sub-contractor support to DoD contracts. Most work is conducted at government site. Some work is completed at contractor site.

**Gap Analysis Findings**
- DAR is deployed on laptops using BitLocker, but not in FIPS mode
- No MFA – using Active Directory
- No centralized auditing solution
- No incident response program

**Solutions to Compliance**
- Reconfigure laptops with FIPS-compliant BitLocker
- Implement Azure Multi-Factor Authentication Server to work with AD FS in Windows Server
- POA&M documented and centralized auditing solution TBD
- POA&M documented, incident response policy drafted and working to contract a MSSP
350 employees. Most sit on contractor site. Full network configured on premise. Manufacture parts for DoD equipment.

**Gap Analysis Findings**
- No continuous monitoring strategy
- No incident response program
- No centralized auditing solution

**Solutions to Compliance**
- POA&M documented and working to deploy Nessus Security Center
- POA&M documented, incident response policy drafted and working to contract a MSSP
- POA&M documented and centralized auditing solution TBD