Workshop on NIST 800-171 Compliance for Alabama DoD Suppliers

2018

Eric Imsand, Ph.D.
Principal Research Scientist
Information Technology & Systems Center
University of Alabama in Huntsville

Brian Tucker
Research Scientist / Program Manager
Office for Operational Excellence
University of Alabama in Huntsville

Joe Paxton
Director
Office for Operational Excellence
University of Alabama in Huntsville

University of Alabama in Huntsville

Joe Paxton
(256) 824-4284
joe.paxton@uah.edu

Eric Imsand
(256) 824-5143
eric.imsand@uah.edu

Brian Tucker
(256) 824-2957
brian.tucker@uah.edu
1. Introduction and Motivation

2. What is the DFARS cyber rule?

3. Overview of CUI

4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing
      Q&A on NIST 800-171r1

5. Overview of UAH Services
   Q&A on Grant Services

6. Sign-Up for Services
Introduction

• This presentation is for anyone who is new to the DFARS Cyber Rule game.
• This presentation will try to give you a broad sense of the following concepts:
  • CUI (& CDI)
  • DFARS Rule 252.204-7012 and NIST SP 800-171r1
  • NIST 800-171r1 Documentation
  • NIST MEP Handbook

• This presentation is NOT geared for people who are already far along in their accreditation
Motivations
Agenda

1. Introduction and Motivation

2. What is the DFARS cyber rule?

3. Overview of CUI

4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing
      Q&A on NIST 800-171r1

5. Overview of UAH Services
   Q&A on Grant Services

6. Sign-Up for Services
What is the “DFARS Cyber Rule”

• In 2015, a change was made to the DFARS to strengthen cyber security
  • Commonly known as “DFARS Cyber Rule”

• New requirements went into effect 12/31/2017

• Bottom line: Contractors have to provide “adequate” cyber security.
  • But who decides what’s adequate?

• NIST has been tasked with defining “adequate”
  • Specifically, you have to implement NIST 800-171r1 (not necessarily “comply”)

• Sort-of Complicated
  • Some requirements spelled out in the DFARS (ex: incident reporting period)
  • Most requirements described in NIST 800-171r1
DFARS Cyber Security Requirements

- DFARS spells out a bunch of requirements
- Spread out over two documents...
  - NIST 800-171r1
  - DFARS 252.204-7012
How does this fit together?

• The DFARS 7012 regulation requires contractors to:
  1. Meet NIST SP 800-171r1 specification
  2. Make certain any **cloud applications** that may store unencrypted CUI/CDI meets the **FedRAMP Moderate** standard (must be equivalence; doesn’t have to be accredited)
  3. Your organization is prepared to respond and report an incident within 72 hours
     • This means you need to obtain an ECA PKI for logging into the appropriate system to report it
     • FSOs generally have this digital token for accessing JPAS system
  4. Your organization has flowed down this same requirement to your subcontractors (if they will also be handling or creating CUI/CDI)

• All Federal Contractors must already meet these requirements; you are at risk of losing existing DoD contracts until you are compliant with these requirements
Scope of DFARS Cybersecurity Rule

• In short, you need to worry about DFARS & NIST 800-171r1 IF:
  • You are a government contractor (for any agency)
    • EVEN IF YOU ARE A SUBCONTRACTOR
  • Handling CUI information on your equipment or in your facility

• “What if I manage a facility, and all the CUI data remains at that facility”
  • “Performance of the Contract”
  • This could go either way.
  • Ask your customer.

• What about subcontractors? Suppliers?
  • Requirements flow down to them.
  • Exceptions for “COTS” products.
  • As the prime, you are responsible for their compliance
How is this being enforced?

• Companies with existing DoD contracts
  • Mixed bag
  • Hearing reports of some contracting officers requesting proof of compliance
    • NIST 800-171r1 System Security Plans (SSPs) and Plan of Actions (POA)
  • DCMA performing some documentation checks
  • Some government agencies haven’t started reviewing (“We should be, but we’re not.”)
How is this being enforced?

• New contracts
  • Some more concrete guidance available for government agencies.
  • DoD has completed a Request for Comments on DARS-2018-0023-0002: Assessing the State of a Contractor’s Information Systems 4-18-2018 (3).


  • Details how contracting officers will incorporate NIST 800—171r1 into future procurements.

---

ASSESSING THE STATE OF A CONTRACTOR'S INTERNAL INFORMATION SYSTEM IN A PROCUREMENT ACTION

<table>
<thead>
<tr>
<th>OBJECTIVE</th>
<th>SOLICITATION/RFP</th>
<th>SOURCE SELECTION</th>
<th>CONTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Evaluate implementation of NIST SP 800-171* at source selection</td>
<td>• DFARS Provision 252.204-7008</td>
<td>• DFARS Clause 252.204-7012</td>
<td>• DFARS Clause 252.204-7012</td>
</tr>
<tr>
<td>Alternative 1A: Go/No Go decision based on implementation status of NIST SP 800-171*</td>
<td>• RFP (e.g., Section I) must require delivery of NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action with the contractor's technical proposal</td>
<td>• Evaluate NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action in accordance with Section M (See Resources: DoD Guidance for Reviewing System Security Plans)</td>
<td>• Incorporate NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action as part of contract</td>
</tr>
<tr>
<td></td>
<td>• RFP (e.g., Section I) must require delivery of NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) with the contractor’s technical proposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RFP (e.g., Section I) must require delivery of NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action with the contractor’s technical proposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RFP (e.g., Section M) must identify requirements for an “Acceptable” (Go/No Go threshold) rating. (See Resources: DoD Guidance for Reviewing System Security Plans)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is my Responsibility?

1. Implement NIST 800-171r1
   - Create a System Security Plan
   - Create a Plan of Action

2. Comply with DoD cyber reporting requirements described in DFARS 252.204-7012

3. Make sure everyone you exchange data with is compliant
   - Subcontractors
   - Cloud providers
   - Other business partners
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?

3. **Overview of CUI**

4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing
      Q&A on NIST 800-171r1

5. Overview of Grant Services
   Q&A on Grant Services

6. Sign-Up for Services
• Controlled Unclassified Information is the new US Gov’t catch-all term for “sensitive but unclassified”.
  • It’s meant to supersede, or possibly replace, FOUO, SBU, LES, etc.

• Markings
  • Previously FOUO becomes CUI ITAR or CUI FOUO

• Basically information that is not technically classified, but is still considered sensitive.

• Who decides if something is CUI?
  • Hopefully spelled out in your contract
  • Rule of thumb: “Performance of the Contract”
  • The government has final decision on this.
  • Different agencies have different outlooks on what constitutes CUI.
  • Ask your customer - the Government Contracting Officer of that contract is the authority
Scope of DFARS Cybersecurity Rule

• Which systems do I have to make more secure?
  • **Anything that:**
    • Stores,
    • Processes,
    • or Transmits CUI.
    • And anything/anyone that comes in contact with those systems.
  • **Other possibilities:**
    • Systems that contain information *about* the work.
    • i.e. financial details, contracts/SOW, etc.
    • Anything related to the “performance of the contract”
Do All Computers Need to Meet NIST 800-171r1?

• Any system involved in producing CUI needs to comply with DFARS/NIST 800-171

• What about computers that are not used to store, process, or transmit CUI?
  • Ex: The receptionist’s computer?
  • Ex: Guest WI-FI?!?

• Answer: where are your network boundaries?
  • If a computer can “talk to” a system that is handling CUI, it has to comply with NIST 800-171r1.
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing
      Q&A on NIST 800-171r1
5. Overview of Grant Services
   Q&A on Grant Services
6. Sign-Up for Services
• NIST = National Institute of Standards and Technology
  • Federal agency
  • Part of the US Department of Commerce

• Officially(?), NIST is responsible for US government cyber security standards
  • NIST has top-flight cyber expertise
  • Responsible for the approval and publication of cryptographic standards, software security procedures, and many other good things.

• In 2015, NIST published the first version of Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

• In short, NIST 800-171r1 is the list of things that you need to do to achieve “adequate” cyber security.
NIST SP 800-171r1

- NIST 800-171r1 is a collection of cyber security “controls”
  - 110 controls, organized into 14 groups
- The Information System (IS) is evaluated against all 110 controls.
- Each control is rated *implemented*, *not implemented*, or *not applicable*
- Two controls require you to produce documents:
  - 3.12.2: “Develop... plans of action...”
  - 3.12.4: “Develop... a system security plan...”
- Fine print:
  - “NIST 800-171 compliant” occurs when all 110 controls are “implemented”
  - “NIST 800-171 implemented” occurs when you assess your InfoSys against 800-171 and document the findings (in the SSP and POA)
NIST SP 800-171r1

• System Security Plan (SSP)
  • Document containing certain required information about the system that contains the CUI (“Controlled Unclassified Information”).

• Plan of Action (PoA)
  • A formal document describing any security problems, how you will solve them, and when you will solve them.

• NOTE: There are other documents that you will create, e.g. Incident Response Plan

• Both of these documents can (and probably will) be requested by the government.
  • If not now, then soon
NIST SP 800-171r1

• NIST 800-171r1 can be summarized as follows:
  • Make sure companies have a reasonable cyber security plan and an incident response plan
  • Make sure that plan is structured and disciplined
    • Procedures
    • Policies
    • Audits to ensure compliance
  • Provide enough flexibility to allow customization
  • Provide documentation to back-up your claims

• Except for a few cases, very few requirements are written as “Thou shalt do ___”
• Most rules have broad objectives you must satisfy
  • Ex: Multi-factor authentication
NIST 800-171r1 Certification

• **You will self-certify**
• In the future, you will be required to submit your compliance package to bid on new contracts
  • Guidance is being drafted for DoD Contracting Officers on how to evaluate NIST 800-171 packages
• You may be audited by the Defense Contract Management Agency (DCMA)
• Correctly completing these documents will achieve DFARS compliance
  • DoD Contractors are required to be DFARS compliant NOW. There is no grace period.
• However, you aren’t NIST SP 800-171 compliant until you meet all 110 of the controls; Currently, there is no deadline for meeting NIST SP 800-171. Stay tuned.
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
      2. Plan of Action
      3. Cloud Computing
         Q&A on NIST 800-171r1
5. Overview of Grant Services
   Q&A on Grant Services
6. Sign-Up for Services
System Security Plan

- Essentially a description of your system
- The plan has three parts:
  - System Identification
  - System Environment
  - Requirements
- NIST has a template available at:
- Your Organization should consider creating a formal, higher level, SSP & Plan of Action that will be turned in for Proposals, etc. and a more detailed “day-to-day” set that is used to drive toward compliance; update the formal one whenever a control gap has been mitigated
SSP Guidance: NIST MEP Handbook

- NIST has published the *NIST MEP Cybersecurity Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*.

- Designed to be a helpful guide for walking through NIST 800-171.

- Currently 170 pages.
  - In a way, this is good.
  - The bare requirements are very terse. How do you know you’ve achieved compliance?
System Security Plan: System Identification

• Basic Information
  • System Name
    • System Categorization (typically *Moderate Impact for Confidentiality*, as defined by FIPS 199)
    • System Unique Identifier (something more specific than “Bob’s Computer”)
  • Responsible Organization
    • Information Owner (Gov’t POC)
    • System Owner (POC responsible for security)
    • System security officer (Security POC)
  • Description (i.e. “purpose” of the system)
    • Include number of end users and privileged users
  • Description of the CUI
    • Types of CUI processed, stored, or transmitted by this system.
System Security Plan: System Environment

• Include both a picture and paragraph describing the system environment

• Need to hit the conceptual high points
  • Don’t include each and every workstation.
  • Do include at least one example of every type of device (and OS)
  • So... include 1 Windows workstation, 1 Mac workstation, 1 iPhone, 1 Android tablet, etc.

• Don’t forget networking equipment

• Idea is to show system boundaries and “interconnections” (i.e. network connections)

• Also need some raw data
  • List of all hardware
  • List of all software (with version)

• Description of ownership and maintenance of your software/hardware
System Environment

Corporate Network-Moderate

- Obi-Wan
- Next-Gen Firewall

MOD-1

Guest Network-Low

- Guest Wi-Fi

VM-3

Windows Workstation (x20)

Corporate Wi-Fi

Linux Workstation (x5)

NP-7
System Security Plan: Requirements

• Actual list of NIST SP 800-171 requirements
• For each item, choose “Implemented”, “Not Implemented”, or “Not Applicable”
• For each item that is “Implemented”, describe the implementation
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
      3. Cloud Computing
         Q&A on NIST 800-171r1
5. Overview of Grant Services
   Q&A on Grant Services
6. Sign-Up for Services
Plan of Action

• Basically a document that states how you’re going to get in compliance
• States the following
  • Each weakness
  • Who’s responsible for fixing it
  • Estimated resources
  • Completion Date
  • Interim milestones
  • Changes to milestones
  • How was the weakness identified
  • Status
• Obviously needs to be updated over time.
• Ideally things will progress from “No” and “Partial” to “Yes”
• NIST has a template available
Plan of Action Example

<table>
<thead>
<tr>
<th>Weaknesses</th>
<th>Responsible Office/Organization</th>
<th>Resource Estimate (funded/unfunded/reallocation)</th>
<th>Scheduled Completion Date</th>
<th>Milestones with Interim Completion Dates</th>
<th>Changes to Milestones</th>
<th>How was the weakness identified?</th>
<th>Status (Ongoing or Complete)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
3. Cloud Computing
   Q&A on NIST 800-171r1
5. Overview of Grant Services
   Q&A on Grant Services
6. Sign-Up for Services
Cloud Computing

• DFARS has two different cloud security guidelines
  • One for companies providing cloud services to the government.
  • Another for companies using commercial cloud services to perform CUI-related work.
• Assuming the latter.
Cloud Computing

• DFARS requires the use of FedRAMP Moderate *equivalent* cloud providers.
  • You do not *have* to use a certified provider.
• Most of the big commercial cloud providers are already certified.
  • Microsoft Azure
  • Amazon AWS
  • Google G Suite and Services
  • Among others
• Full list at [https://www.fedramp.gov/](https://www.fedramp.gov/)
• Important: How is this cloud provider part of your IS? (SaaS, IaaS, etc.?)
• NOTE: You still have to manage cloud accounts per NIST 800-171r1
  • i.e. Multi-factor authentication, separation of duties, etc.
Other DFARS “gotchas”

• Items covered by the DFARS *but not in NIST 800-171r1*.
• Not necessarily documentation issues, but things that surprise folks

• Reporting
  • What if you discover that you have an incident?
  • You **have** to report it within **72 hours**.
  • Expected to provide an incident report
    • **THIS MEANS YOU SHOULD HAVE AN INCIDENT RESPONSE PLAN**

• Monitoring
  • There are requirements for monitoring.
  • It will be hard to support your SSP if you cannot document any monitoring.
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing

Q&A on NIST 800-171r1

5. Overview of Grant Services
   Q&A on Grant Services

6. Sign-Up for Services
Agenda

1. Introduction and Motivation
2. What is the DFARS cyber rule?
3. Overview of CUI
4. NIST SP 800-171r1
   1. System Security Plan (including Assessment)
   2. Plan of Action
   3. Cloud Computing
      Q&A on NIST 800-171r1
5. Overview of Grant Services
   Q&A on Grant Services
6. Sign-Up for Services
OEA Objective in Correlation to DoD Supply Chain Resiliency

• OEA Mission
  • DoD Industrial base resiliency
  • Economic Security and National Security

• Alabama Cybersecurity Grant
  • Education – Workshops across the state of Alabama
  • Support – Using NIST 800-171r1 guidelines, provide coaching and support in conducting assessments, developing gap reports and assisting in the development of system security plans and action plans toward achieving compliance as allowed by the grant funding.
NIST 800-171 R1 IMPLEMENTATION

**Grant services**
- **Assessment**: Conduct Assessment to NIST SP 800-171 and define system gaps
- **Plan of Action**: Develop Plan of Action and Milestones (POAM) to close gaps
- **System Security Plan**: Develop/Update System Security Plan (SSP)

**Execution**
- Execute Plan of Action and Milestones and Update SSP

READY FOR IMPLEMENTATION
TO BE NIST 800-171 COMPLIANT
ACCESS Grant Services Provided

**Education (FREE)**
- Pre-Workshop Questionnaire available online through the OOE website
- Workshop a two hour educational session on NIST 800-171r1 compliance

**Assessment & Gap Report (Company Co-pay $350)**
- Assessment interactive and comprehensive evaluation of NIST 800-171r1 cybersecurity controls
- Gap Report gap reports show businesses detailed needs for improvement based on assessment results

**Planning Development Support (Additional Company Co-pay $1,500)**
- Plan of Action and Milestones action plan to close cybersecurity gaps within a business
- System Security Plan construction / enhancement of a custom system security plan

**READY FOR IMPLEMENTATION TO BE NIST 800-171 COMPLIANT**

**TODAY**

**SIGN UP TODAY**

**POST ASSESSMENT**
Assessment and Gap Report Services

The Process

- Kickoff visit / call
- Pre-Assessment Questionnaire
- Pre-Assessment Feedback
- Complete Assessment
- Complete and Review Gap Report

TO GET STARTED...

Before you leave today...
- Pre-Workshop survey submitted
- Sign-up today
- Schedule initial call to review process

Next Steps...
- Conduct Initial Call with UAH
- Sign UAH Agreement for company $350 co-pay
• What have we talked about?
  • DFARS requires “adequate” cyber security. You achieve “adequate” security by implementing NIST 800-171r1.
  • NIST 800-171r1 requires (minimum) two documents:
    • SSP: System Security Plan
    • Plan of Action
  • NIST provides templates for these documents
  • “NIST MEP Cybersecurity Self-Assessment Handbook”

• UAH has services available to help your organization implement NIST 800-171r1.
  • First step is complete survey and sign-up
  • Schedule initial call
For more information

Brian Tucker  
University of Alabama in Huntsville  
Office for Operational Excellence  
ACCESS Program Manager  
256.824.2957  
brian.tucker@uah.edu

www.uah.edu/ooe/access
Resources Available

At least the following resources are available on the UAH OOE Access Program Resource Page:

- NIST Special Publication SP 800-171 rev 1
- NIST Handbook 162
- NIST 800-171 SSP Template
- NIST 800-171 Plan of Action Template

Link to ACCESS Program Resources
Backup Slides
SSP Guidance: NIST MEP Handbook

• For example, NIST 800-171r1 Requirement 3.5.8:
  • **Original:** “Prohibit password reuse for a specified number of generations.”
  • **MEP Handbook:**
    • *Can passwords be re-used after a certain number of days or a defined number of password changes?*
      • Yes  No  Partially  Does Not Apply  Alternative Approach
    • *Can users re-use the same password when changing their password for at least a certain number of changes?*
      • Yes  No  Partially  Does Not Apply  Alternative Approach
    • *Is password reuse prohibited for a defined number of generations?*
      • Yes  No  Partially  Does Not Apply  Alternative Approach
    • *Are passwords unique to the organization’s systems and not re-used on external information systems?*
      • Yes  No  Partially  Does Not Apply  Alternative Approach
Plus, the MEP Handbook gives you some guidance into why you’re doing this:

• “The reuse of passwords can greatly diminish the effectiveness of authentication security requirements on the system. While many users may find it convenient to reuse the same password on various systems, this practice can increase the risk of a security incident.”

As well as guides for figuring out if you are in compliance.

• Where to Look:
  • identification and authentication policy
  • password policy procedures addressing authenticator management
  • Etc.

• Who to Talk to:
  • employees with authenticator management responsibilities
  • employees with information security responsibilities
  • system/network administrators