Briefing Overview

Content Structure

- Define DFARS 252.204-7012
  - Controlled Defense Information
  - Contractor Internal System
  - Adequate Security Defined

- Define NIST SP 800-171
  - Requirements Overview
  - Required Deliverables
  - Impact of non-compliance / teeth

- Recommendations
  - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
  - Sample Recommendations

- Conclusion
  - Key Take-Aways

Intent

✓ Achieve understanding of the DFARS requirement
✓ Achieve understanding of how to achieve compliance with DFARS
✓ Identify industry “best practices” for becoming compliant
DFARS Clause 252.204-7012 requires contractors / sub-contractors to:

1. Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor’s internal information system or network
2. Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor’s ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. Submit media (if requested) and additional information to support a damage assessment
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.
Covered defense information means:

1. Unclassified controlled technical information (CTI) or other information as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with the law, regulations, and government-wide policies and is –
   a. Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR
   b. Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.*

* In support of the performance of the contract is not meant to include the contractor’s internal information (e.g., human resources or financial) that is incidental to the contract performance.
What Information Do You Need to Protect?

Contractor’s Internal System
- Federal Contract Information
- Controlled Unclassified Information
- Covered Defense Information
  - Includes Unclassified Controlled Technical Information

DoD Owned and/or Operated Information System
- Internal Cloud NIST SP 171
- External SP Equivalent to FedRAMP Moderate

System Operated on Behalf of the DoD
- Controlled Unclassified Information

Cloud Service Provider
- When cloud services are used to process data on the DoD’s behalf, DFARS clause 252.239-7010 and DoD Cloud Computing SRG apply
- When cloud services are provided by DoD, the DoD Cloud Computing SRG apply
Adequate Security Defined

- DFARS 252.204-7012  (b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

  - (b)(2)(ii)(A): The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017 Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.
Briefing Overview

Content Structure

- Define DFARS 252.204-7012
  - Controlled Defense Information
  - Contractor Internal System
  - Adequate Security Defined

- Define NIST SP 800-171
  - Requirements Overview
  - Required Deliverables
  - Impact of non-compliance / teeth

- Recommendations
  - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
  - Sample Recommendations

- Conclusion
  - Key Take-Aways

Intent

- Achieve understanding of the DFARS requirement
- Achieve understanding of how to achieve compliance with DFARS
- Identify industry “best practices” for becoming compliant
NIST SP 800-171 Requirements

- Details the security requirements to protect confidentiality of **Federal Contract Information, CDI, or CUI** on non-Federal information systems.

- Acts as a non-tailorable baseline, but offers flexibility in how to meet requirements.

- Most requirements focus on policy, process, and configuring IT securely, but a number of controls may require security-related software or hardware.
For ease of use, the security requirements are organized into 14 control families.
Each family contains the requirements related to the general security topic of the family, and contain a total of 110 individual controls/requirements.
To document implementation of NIST SP 800-171, companies should have a system security plan in place, in addition to any associated plans of action:

  - Develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

  - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

* The contractor self-attests (by signing contract) to be compliant with DFARS Clause 252.204-7012, to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the system security plan and associated plans of action).
DARS-2018-0023-0002

“Assessing the State of a Contractor's Internal Information System in a Procurement Action” has been provided to illustrate how DoD may choose to assess submitted SSPs and POA&Ms in procurement actions that require the implementation of NIST SP 800-171.
1. Evaluate implementation of NIST SP 800-171 at source selection
   - Alternative 1A: Go/No-Go Decision based on status of NIST SP 800-171 compliance
   - Alternative 1B: Assess NIST SP 800-171 implementation as a separate technical evaluation factor
2. Require protections in addition to the security requirements in NIST SP 800-171 and evaluate at source selection
3. Assess/Track implementation of NIST SP 800-171 security requirements after contract award
   - The government may also monitor compliance of NIST SP 800-171 (e.g. MDA CAT)
4. Contractors “self-attest” to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171
Briefing Overview

Content Structure

• Define DFARS 252.204-7012
  • Controlled Defense Information
  • Contractor Internal System
  • Adequate Security Defined

• Define NIST SP 800-171
  • Requirements Overview
  • Required Deliverables
  • Impact of non-compliance / teeth

• Recommendations
  • DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
  • Sample Recommendations

• Conclusion
  • Key Take-Aways

Intent

✓ Achieve understanding of the DFARS requirement
✓ Achieve understanding of how to achieve compliance with DFARS
✓ Identify industry “best practices” for becoming compliant
Recommendations

**DoD Guidance for Reviewing SSPs and the NIST SP 800-171**

**Security Requirements Not Yet Implemented**

<table>
<thead>
<tr>
<th>NIST SP 800-171 Security Requirement</th>
<th>Corresponding NIST SP 800-53 Security Controls</th>
<th>NIST Priority</th>
<th>DoD Value (High - Mod - Low)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.4 Separate the duties of individuals to reduce the risk of malicious activity without collusion.</td>
<td>AC-3 Separation of Duties</td>
<td>P1</td>
<td>5/5</td>
<td>METHODS TO IMPLEMENT: IT configuration vulnerability. For businesses with a small number of information technology personnel to separate duties, risk may be assessed at level 3 if the company has few IT assets to manage.</td>
</tr>
<tr>
<td>3.1.5 Employ the principle of least privilege, including for specific security functions and privileges.</td>
<td>AC-6 Least Privilege</td>
<td>P1</td>
<td>5/5</td>
<td>METHODS TO IMPLEMENT: IT configuration. For businesses with a small number of information technology personnel to separate duties, risk may be assessed at level 3 if the company has few IT assets to manage.</td>
</tr>
<tr>
<td>3.1.6 Use non-trusted accounts or roles when accessing non-critical functions.</td>
<td>AC-6(R) Least Privilege (Non-privileged Access to Non-critical Functions)</td>
<td>P1</td>
<td>5</td>
<td>METHODS TO IMPLEMENT: IT configuration. For businesses with a small number of information technology personnel to separate duties, risk may be assessed at level 3 if the company has few IT assets to manage.</td>
</tr>
<tr>
<td>3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.</td>
<td>AC-6(D) Least Privilege (Allowing Use of Privileged Functions)</td>
<td>P1</td>
<td>5</td>
<td>METHODS TO IMPLEMENT: IT configuration. For businesses with a small number of information technology personnel to separate duties, risk may be assessed at level 3 if the company has few IT assets to manage.</td>
</tr>
<tr>
<td>3.1.8 Limit unsuccessful login attempts.</td>
<td>AC-7 Unsuccessful Login Attempts</td>
<td>P1</td>
<td>2</td>
<td>METHODS TO IMPLEMENT: IT configuration. For businesses with a small number of information technology personnel to separate duties, risk may be assessed at level 3 if the company has few IT assets to manage.</td>
</tr>
</tbody>
</table>

**Two key artifacts should guide your efforts**

- With limited time and resources, organizations may want to prioritize which controls to enact first as well as determine which controls may be implemented internally and which may require outside assistance.
Recommendations

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

- “NIST SP 800-53 priority codes were considered in the calculation of the DoD Implementation Value for corresponding NIST SP 800-171 security requirements.”
- “DoD Values range from 5 - representing the highest impact on the information system, or highest priority to implement, to 1 - representing the lowest impact on the information system, or lowest priority to implement.”
- “The DoD Value for NIST SP 800-171 security requirements are typically 5, but may range between 5 and 3.”
- “The guidance is not to be used to assess implemented security requirements, nor to compare or score a company’s approach to implementing a security requirement.”

“Where necessary, posters or other printed materials may be used in lieu of an automated system banner.” NIST SP 800-171R1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Appendix F, Discussion on 3.1.9, p71.
Sample Recommendation

- “Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.” NIST SP 800-171R1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Appendix F, Discussion on 3.1.21, p75.
- Even though this control is rated at a “5,” the guidance shows that only a policy is required.
- Technical limitations/ configurations (e.g. Iron Key) are not required for this particular requirement.
Free Basic Insider Threat Training: [www.cdse.edu/catalog/elearning/INT101.html](http://www.cdse.edu/catalog/elearning/INT101.html)

“Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations). NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.1.9, p76.

Free In-Depth Insider Threat Training: [www.cdse.edu/catalog/insider-threat.html](http://www.cdse.edu/catalog/insider-threat.html)
“Policy enforcement methods include procedural methods, automated methods, or both.” NIST SP 800-171R1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Appendix F, Discussion on 3.4.9, p83.

Even though this control is rated at a “5,” the guidance shows that only a policy is required.

Information systems can be configured to automatically deny user-installed software, but this can be probative to organizations like software developers.
Vulnerability scanning includes, for example: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.” NIST SP 800-171R1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Appendix F, Discussion on 3.11.2, p97.

- This control requires additional tools.
- The requirement may require outside assistance to define routine scan frequencies, configure scan utilities, and interpret scan results.
- Market is quickly evolving, and very cost effective and proven tools are now available (e.g., MARS Box)
“DFARS Compliance” incorporates more than just following a simple DFARS clause
– It encompasses protecting by implementing security controls established by NIST 800-171 and
abiding by DFARS252.204-7012 in terms of protection and incident reporting

There’s a lot to do: Identifying Federal Contract Information, CDI, or CUI, determining which of the 110
NIST 800-171 Controls aren’t in place in an SSP, planning for their remediation in a POA&M, and then
actually implementing the controls

All organizations have the opportunity to implement the requirements in-house, or they can contract
out work to a third party to support a compliance assessment, policy development, architecture
updates, or on-going monitoring.

Depending on the complexity of your organization should drive this decision-making
Questions

For more information about Mission Multiplier, please visit us at: www.missionmultiplier.com
Reference Slides
Cyber Incident Reporting

DFARS 204.7302 (d)

A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

- Contractors / sub-contractors must submit a cyber incident report via https://dibnet.dod.mil/
- Upon receipt of a cyber incident report –
  - DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s)
  - The contracting officer(s) provides the report to the requiring activities
  - DC3 analyzes report to identify cyber threat vectors and adversary trends
  - DCS contacts the reporting company if the report is incomplete
Cyber Incident Reporting
When should DFARS clause 252.204-7012 flow down to sub-contractors?

- The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information.
- The contractor shall determine if the information required for subcontractor performance is, or retains its identity as, covered defense information and requires safeguarding.
- Flow down is a requirement of the terms of the contract with the government, which must be enforced by the prime contractor as a result of compliance with these terms.
  - If a sub-contractor does not agree to comply with the terms of DFARS clause 252.204-7012, then covered defense information shall not be shared with the sub-contractor or otherwise reside on its information system.

The DoD’s emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flow down of information requiring protection.
Resources

- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information
  - This document is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in SP 800-171, *Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations*

- Cybersecurity Evaluation Tool (CSET)
  - No-cost application, developed by DHS’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control systems and IT network security practices

- NIST MEP Handbook Cybersecurity Handbook (HB-162)
  - Handbook provides a step-by-step guide to assessing a small manufacturer’s information systems against the security requirements in NIST SP 800-171, rev 1, *"Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations”*
  - [https://www.nist.gov/mep](https://www.nist.gov/mep)