Cybersecurity Resiliency for Defense Contractors Webinar Series:

DFARS NIST 800-171 Compliance Process

October 22, 2020
Jana White

ALPINE SECURITY IMEC

1

Today's Topics

- Focus on how to become compliant with DFARS 800-171
- What is CUI or CDI?
- Assessment: NIST 800-171A: 110 controls
- Documents of Compliance: System Security Plan, Plan of Actions and Milestones, Incident Response Plan

ALPINE SECURITY IMEC

2

ALPINE SECURITY

Service-Disabled Veteran Owned Small Business (SDVOSB)

Areas of Focus:

Cybersecurity Training

Penetration Testing

Vulnerability Assessments

CISO-as-a-Service

Cybersecurity Strategy

DFARS 252.204-7012 & CMMC

Based in Greater St. Louis Area

IMEC

3

Focus on how to become compliant with DFARS 800-171

1. Don't panic!
2. Use an assessment tool
3. Gather all your materials/artifacts for review
4. Conduct the assessment
5. Determine the gap
6. Develop your remediation plan (POAM)
7. Take action (remediate)!

ALPINE SECURITY

IMEC

4

NIST SP 800-171 r2 Review

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

- 110 Controls, 14 Control Families
- DFARS Compliance Requirement

ALPINE SECURITY

IMEC

5

The Three Control Types

- **Management controls:** The security controls that focus on the management of risk and the management of information system security
- **Operational controls:** The security controls that are primarily implemented and executed by people (as opposed to systems)
- **Technical controls:** The security controls that are primarily implemented and executed by the system through the system's hardware, software, or firmware

ALPINE SECURITY

IMEC

6

Control Families in 800-171

- 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

ALPINE SECURITY

IMEC

7

What is CUI or CDI?

In its most basic form, any contract or part of a contract that has come from the federal government (originally from the government, it may come from anywhere in the supply chain above you as well) is considered CUI. CUI is:

1. Information the Government creates or possesses that is protected by law, regulation, or government-wide policy
   -Example: DoD work products and emails
2. Information that an entity creates or possesses for or on behalf of the Government that is protected by law, regulation, or government-wide policy
   -Example: information associated with DoD contracts

DoD (in final rule October 4, 2016) narrows the definition of CDI to only two categories: (1) CTI and (2) CUI

ALPINE SECURITY

IMEC

8

Become a CUI archaeologist!

- Examine all servers, workstations, and other devices
- Examine all email accounts
- Check for portable media and backups
- Don't forget about physical documents (blueprints, schematics, printed contracts)

ALPINE SECURITY

IMEC

9

Assessment: NIST 800-171A: 110 controls

The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards intended to meet the set of security requirements specified in NIST Special Publication 800-171.

Evidence needed to determine compliance comes from the implementation of the selected safeguards to satisfy the CUI security requirements and from the assessments of that implementation.

ALPINE SECURITY

IMEC

10

800-171A Assessment Example

3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.3[a] *information flow control policies are defined.*
	3.1.3[b] *methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c] *designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d] *authorizations for controlling the flow of CUI are defined.*
	3.1.3[e] *approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI SECURITY REQUIREMENT

ALPINE SECURITY

IMEC

11

What does DFARS self-attestation mean?

The DoD interprets "self-attestation" as admission of compliance, and "implementation" of NIST SP 800-171 as having a completed Systems Security Plan (SSP) and a Plan-of-Action and Milestones (POA&M)

ALPINE SECURITY

IMEC

12

DFARS Compliance Intended Due Date

From DFARS 252.204-2008 -

- (c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—
- (1) By submission of this offer, the **Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171** "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer **not later than December 31, 2017**.

IMEC

13

False Claims Act

Liability for any person who knowingly submits a false claim to the government or causes another to submit a false claim to the government or knowingly makes a false record or statement to get a false claim paid by the government

- *An SSP/POAM may misrepresent a contractor's actual cybersecurity status, and the DoD may take action based on the misrepresentation of compliance. The DoD can establish that the cybersecurity status of a contractor was included in the award decision, and this could put existing and future contracts at risk*

ALPINE SECURITY

IMEC

14

What if the DoD wants to determine my 800-171 compliance?

- DoD may require the Defense Contract Management Agency (DCMA) to verify that the contractor has an SSP and POA&M, and conduct a compliance assessment for the 800-171 controls
  - *Primes and Tier 1*
  - *Be prepared, just in case*
  - *DFARS Case 2019-D041**

ALPINE SECURITY

IMEC

15

What is the two-prong test?

Testing the compliance of a control using two of the standard assessment methods: examine, interview, and test.

- The **examine** method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities)
- The **interview** method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence
- The **test** method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior

ALPINE SECURITY

IMEC

16

Is a policy document enough to prove compliance?

ALPINE SECURITY

IMEC

17

The Upcoming Interim Rule (DFARS Case 2019-D041) *New*

DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

Effective November 30, 2020

ALPINE SECURITY

IMEC

18

NIST SP 800-171 DoD Assessment Methodology *New*

- The NIST SP 800-171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204-7012
- Provides DoD with visibility into the scores of assessments, **verifies that a contractor has a current assessment (3yrs or less) on record prior to contract award**

ALPINE SECURITY

IMEC

19

Cybersecurity Scoring Levels of the NIST 800-171 Assessment Methodology

- The DoD 800-171 Assessment Methodology also describes three levels of "confidence" in the results of the NIST assessment:
  - ***Basic (Low):*** *contractor self-assessment of SSP using Methodology*
  - ***Medium:*** *DoD review of SSP using Methodology*
  - ***High:*** *DoD thorough on-site review of SSP and the execution (verification/examination/demonstration) of contractor's system security plan and implementation of the NIST SP 800-171 security requirements*

ALPINE SECURITY

IMEC

20

Supplier Performance Risk System (SPRS)

- The results of NIST SP 800-171 DoD Assessments are documented in the Supplier Performance Risk System (SPRS) at https://www.sprs.csd.disa.mil/

ALPINE SECURITY IMEC

21

What is an Information System?

NIST defines an information system (IS) as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Your CUI information system (IS) is the subset of your network and environment (includes hardware, software, and physical and/or logical boundaries) that is used to receive, store, use, and transmit CUI.

Your SSP and POAM are used to document and define your CUI IS and its current compliance and security status.

ALPINE SECURITY IMEC

22

How do I define my CUI Information System?

- Identify where CUI enters your organization (email, vendor portals, registered mail)
- Identify where you store CUI (servers, workstations, laptops, mobile devices, backups)
- Identify where you send CUI (email, vendor purchase orders, vendor portals)
- Diagram it!!!!

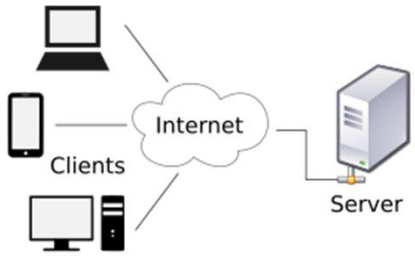
ALPINE SECURITY

IMEC

23

CUI Diagramming Tips

- Use existing network diagrams as a starting point
- Keep it as simple as possible
- Ensure that physical and logical boundaries are included
- Label everything in the diagram with a unique identifier



ALPINE SECURITY

IMEC

24

Documents of Compliance: System Security Plan, Plan of Actions and Milestones, Incident Response Plan

- Every company should clearly define their CUI Information System (IS)
  - *SSP*
  - *POAM*
- Every company should have an up-to-date Incident Response Plan for cybersecurity incidents
  - *Tested regularly*
  - *Train your CIRT*

ALPINE SECURITY

IMEC

25

System Security Plan (SSP)

For the CUI security requirements in NIST SP 800-171, nonfederal organizations describe in a system security plan, how the specified requirements are met or how organizations plan to meet the requirements

ALPINE SECURITY

IMEC

26

What should be in my SSP?

The plan describes the system boundary; the environment in which the system operates; how the requirements are implemented; and the relationships with or connections to other systems.

ALPINE SECURITY

IMEC

27

Plan of Actions and Milestones (POAM)

For the CUI security requirements in NIST SP 800-171, the POAM identifies tasks needed to achieve compliance for each of the 800-171 controls that are not currently implemented or compliant.

ALPINE SECURITY

IMEC

28

What should be in my POAM?

The POAM details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

ALPINE SECURITY

IMEC

29

Incident Response Plan (IRP)

Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability.

ALPINE SECURITY

IMEC

30

What should be in my IRP?

- Organizations should document their guidelines for interactions with other organizations regarding incidents. (who, how, when)
- Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. (containment, training)
- Organizations should emphasize the importance of incident detection and analysis throughout the organization. (continuous monitoring)
- Organizations should create written guidelines for prioritizing incidents. (based on risk)

ALPINE SECURITY

IMEC

31

NIST Cybersecurity Incident Handling References

- NIST SP 800-61 Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

ALPINE SECURITY

IMEC

32

DFARS Clause 252.204-7012 – The IRP Booster Shot

- Safeguarding Covered Defense Information and Cyber Incident Reporting (highlights)
  - ***Adequate security*** *(The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017)*
  - *If the Contractor intends to use an external cloud service provider …the* ***Contractor shall require and ensure that the cloud service provider meets security requirements*** *equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline*
  - *Cyber incident reporting requirement (includes review for compromise,* ***Rapidly report cyber incidents to DoD*** *at https://dibnet.dod.mil., **isolate malicious software** in connection with a reported cyber incident*

ALPINE SECURITY

IMEC

33

Keep It Secret, Keep It Safe

The **SSP**, **POAM**, and **IRP** are **highly sensitive** documents listing all of the vulnerabilities and details of your CUI IS. **Keep them secured at all times!**

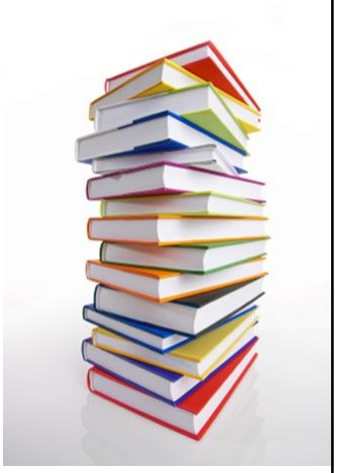
ALPINE SECURITY

IMEC

34

NIST SP 800-171 Compliance Resources

- NIST 800-171 r 2 – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- NIST 800-171A – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf
- NIST 800-53 r4– https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf



ALPINE SECURITY

IMEC

35

Other Helpful Resources (Freebies!)

- DFARS 800-171 Controls Audit Spreadsheet Handout
- SSP and IRP Handout
- POAM Handout

ALPINE SECURITY

IMEC

36

What We Covered Today…

- Focus on how to become compliant with DFARS 800-171
- What is CUI or CDI?
- Assessment: NIST 800-171A: 110 controls
- Documents of Compliance: System Security Plan, Plan of Actions and Milestones, Incident Response Plan

ALPINE SECURITY

IMEC

37

Jana White
jana.white@alpinesecurity.com
www.alpinesecurity.com
info@alpinesecurity.com
(844) 925-7463

ALPINE SECURITY

IMEC

38