Cybersecurity Resiliency for Defense Contractors Webinar Series:

DFARS & CMMC Overview

October 15, 2020
Jana White

ALPINE SECURITY IMEC

1

Today's Topics

- Cybersecurity concepts you need to know
- Why does DFARS exist?
- Current requirements for companies with Controlled Unclassified Information (CUI) or DoD Covered Defense Information (CDI)
- What is CMMC?

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

What Role Do I Play In Cybersecurity?

As a leader, you are responsible for the culture and level of "buy-in" your employees will adopt regarding cybersecurity. If it is important to you, it will be important to them

ALPINE SECURITY

IMEC

4

How Does Cybersecurity Align With My Business Goals?

Goals

helps keep your organization secure so you can achieve your business goals

reduces risk by preventing unauthorized data modification/loss/theft and damage to your brand due to a loss of client confidence

mature cybersecurity practices give you an advantage over your competitors

ALPINE SECURITY

IMEC

5

What is Risk?

- Risk is likelihood of something bad happening to you
- The formula for determining risk is likelihood (what are the odds this thing will happen) multiplied by the impact (how bad will it hurt if it happens)

ALPINE SECURITY

IMEC

6

What Do I Do With Risk Once I Find It?

The goal is to get your organizational risk down to an acceptable level

- *Risk level is determined by highest authority who can accept risk*
- *Laws, regulations, and industry requirements factor into risk acceptance*
  - Insurers may have additional risk related requirements

ALPINE SECURITY

IMEC

7

Where Does The Risk To My Organization Come From?

- People
  - *Social Engineering*
  - *Errors and Mistakes*
  - *Malicious Actions*
- Processes
  - *Shared Accounts*
  - *Insufficient Onboarding/Offboarding Process*
- Technology
  - *Misconfigurations*
  - *Unpatched Systems*
  - *Legacy Devices*

ALPINE SECURITY

IMEC

8

What Am I Trying To Protect?

- Human Life
  - *Employees*
  - *Clients*
  - *Visitors*
  - *Local, National, and Global Communities*
- Company Assets (INCLUDING DATA!)
- Client Assets (INCLUDING DATA!)

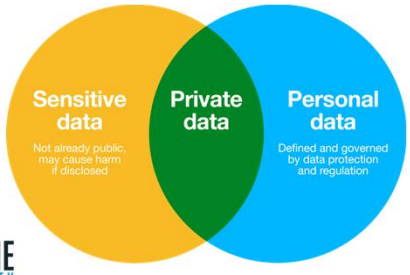
ALPINE SECURITY

IMEC

9

Different Types of Sensitive Data

- Personally Identifiable Information (PII) - any data that can identify a specific individual
- Protected Health Information (PHI) - any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual



ALPINE SECURITY

IMEC

10

Different Types of Sensitive Data Cont.

- Business Information - data that would cause damage to a company if accessed by a competitor or the public (financial data, trade secrets, supplier information, customer data)
- Big Data - large amounts of data that will not fit into a standard (relational) database for analysis and processing

ALPINE SECURITY

IMEC

11

Different Types of Sensitive Data Cont.

- Covered Defense Information (CDI) - Information given to the contractor by, or on behalf of, the DoD for a reason related to performing the stipulations of the contract, or information collected, developed, received, transmitted, used or stored by, or on behalf of, the contractor for reasons related to performing the terms of the contract.
  - *The DoD (Oct 4, 2016) narrows the definition of CDI to only two categories: (1) CTI and (2) CUI. (CDI language contained in DFARS 252.204-7012 intended to align with CUI efforts)*

ALPINE SECURITY

IMEC

12

Different Types of Sensitive Data Cont.

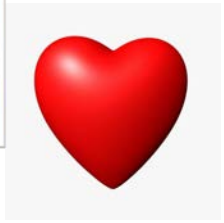
- Controlled Unclassified Information (CUI) - information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended

ALPINE SECURITY

IMEC

13

The Best Type of Data…



ALPINE SECURITY

IMEC

14

Protecting Supply Chain Data: What Should I Be Looking For?

- Third party service providers or vendors with physical or virtual access to information systems, software code, or IP (introduction of malware, exfiltration of data, potential breach point)
- Poor information security practices (no data classification or marking process, no access control, no IRP)
- Compromised software or hardware (ransomware, spyware)

ALPINE SECURITY

IMEC

15

Protecting Supply Chain Data: What Should I Be Looking For? Cont.

- Software security vulnerabilities in supply chain management or supplier systems (misconfiguration, poor patch management)
- Third party data storage or data aggregators (cloud)

ALPINE SECURITY

IMEC

16

How Do I Protect My Data? The CIA Triad

ALPINE SECURITY

IMEC

17

Confidentiality

- Ensures that only authorized people can access sensitive data
  - *Example - Encryption*

ALPINE SECURITY

IMEC

18

Integrity

- Ensures that the data is not manipulated or falsified
  - *Example - Hashing*

ALPINE SECURITY

IMEC

19

Availability

- Ensures authorized subjects are granted timely and uninterrupted access to data
  - *Example - Back-ups*

ALPINE SECURITY

IMEC

20

What is DFARS?

- DFARS (Defense Federal Acquisition Regulation Supplement) is a DoD (Department of Defense)-specific supplement to the FAR (Federal Acquisition Regulation). It provides acquisition regulations that are specific to the DoD
- DoD government acquisition officials and contractors and subcontractors doing business with the DoD must adhere to the regulations in the DFARS

21

Why Does DFARS exist?

- Federal departments and civilian agencies were employing ad hoc, agency-specific policies, procedures, and markings to safeguard and control CUI
- This led to inconsistent, unclear, or unnecessarily restrictive dissemination policies, created impediments to authorized information sharing, and identified serious security concerns

22

Nobody wants to be this guy…

National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare

China's sole operating aircraft carrier leaves Dalian in northeast China for sea trials last month. (Li Gang/Xinhua/AP)

By Ellen Nakashima and Paul Sonne
June 8, 2018 at 2:04 p.m. CDT

ALPINE SECURITY

IMEC

23

Who is NIST, and What is 800-171?

- NIST (National Institute of Standards and Technology) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. (vendor agnostic)
- NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171

NIST

ALPINE SECURITY

IMEC

24

How Does DFARS Apply to Me?

- The cybersecurity requirements under DFARS mandate that DoD contractors and subcontractors must implement controls that are specified in the NIST SP (Special Publication) 800-171
- All contractors and subcontractors processing, storing, or transmitting CUI need to meet minimum security standards specified in the DFARS. Failing to meet these standards can end up in the loss of contracts with the DoD

ALPINE SECURITY

IMEC

25

How Do I Know If I Am DFARS Compliant or Not?

- Conduct a readiness assessment yourself– internal audit (use NIST SP 800-171A)
- Have an independent contractor conduct a readiness assessment

Focus on the gap analysis, develop an action plan to become compliant, take action!

ALPINE SECURITY

IMEC

26

Current requirements for companies with Controlled Unclassified Information (CUI) or DoD Covered Defense Information (CDI)

To meet the minimum requirements, DoD contractors must:

- Provide adequate security to safeguard covered defense information that resides in or transits through your internal unclassified information systems from unauthorized access and disclosure **(Diagram and control CDI/CUI)**
- Rapidly report cyber incidents and cooperate with the DoD to respond to these security incidents, including providing access to affected media and submitting malicious software **(IRP)**
- In order to be considered DFARS compliant, non-federal and contractor information systems/organizations must pass a NIST SP 800-171 readiness assessment **(SSP, POAM)**

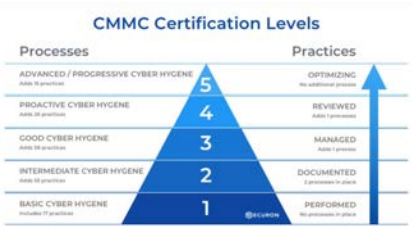
ALPINE SECURITY

IMEC

27

What is CMMC?

CMMC is an acronym for Cybersecurity Maturity Model Certification. The CMMC has five maturity levels that range from "Basic Cybersecurity Hygiene" (Level 1) to "Advanced/Progressive"(Level 5)



The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use **CMMC compliance** as a requirement for contract award

ALPINE SECURITY

IMEC

28

How Will CMMC Apply to Me?

- DOD will use the CMMC framework to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB)
- CMMC will serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place (Target level expected to be level 3)
- Self-assessment will not be an option – assessments must be conducted by CMMC Third Party Assessment Organizations (C3PAOs) or accredited individual assessors
- In general, a CMMC certificate will be valid for 3 years

ALPINE SECURITY

IMEC

29

How Do I Know If I Am CMMC Compliant or Not?

- Conduct a readiness assessment yourself– internal audit (Use CMMC v1.02 or current)
- Have an independent contractor conduct a readiness assessment

Focus on the gap analysis, develop an action plan to become compliant, take action!

ALPINE SECURITY

IMEC

30

Where Can I Go For Help With DFARS or CMMC Compliance?

- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: NIST SP 800-171 r.2 (DFARS controls) – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- Cybersecurity Maturity Model Certification Current Version 1.02 - https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
- Contact your IMEC Representative

ALPINE SECURITY

IMEC

31

Other Helpful Resources (Freebies!)

- Spiceworks IT Asset Management Software - https://www.spiceworks.com/free-asset-management-software/
- CIS RAM (Risk Assessment Method) - https://learn.cisecurity.org/cis-ram

ALPINE SECURITY

IMEC

32

What We Covered Today…

- Cybersecurity concepts you need to know
- Why does DFARS exist?
- Current requirements for companies with Controlled Unclassified Information (CUI) or DoD Covered Defense Information (CDI)
- What is CMMC?

33

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

34