RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **LAW-W02**

The Defense Industrial Base, CMMC, the False Claims Act, and Insider Threat

Joy Beland, CISM | SSAP

Senior Cybersecurity Consultant
Edwards Performance Solutions
@belandjoy
www.linkedin.com/in/joy-belinda-beland

Shawnee Delaney

CEO
Vaillance Group
https://www.linkedin.com/in/shawnee-delaney-30935651/

Ryan Berry, Esq

Partner
Ward & Berry PLLC
https://www.linkedin.com/in/ryanberry/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- Historical Background - CMMC and the DIB: Joy Beland
- False Claims Act | Whistleblowers: Ryan Berry
- Insider Threat & The Critical Pathway: Shawnee Delaney

Sensitivity of Shared Data

FCI – Federal Contract Information

Contracts issued by the acquisition team acting on behalf of the DoD.

Contracts contain sensitive information.

CUI – Controlled Unclassified Information

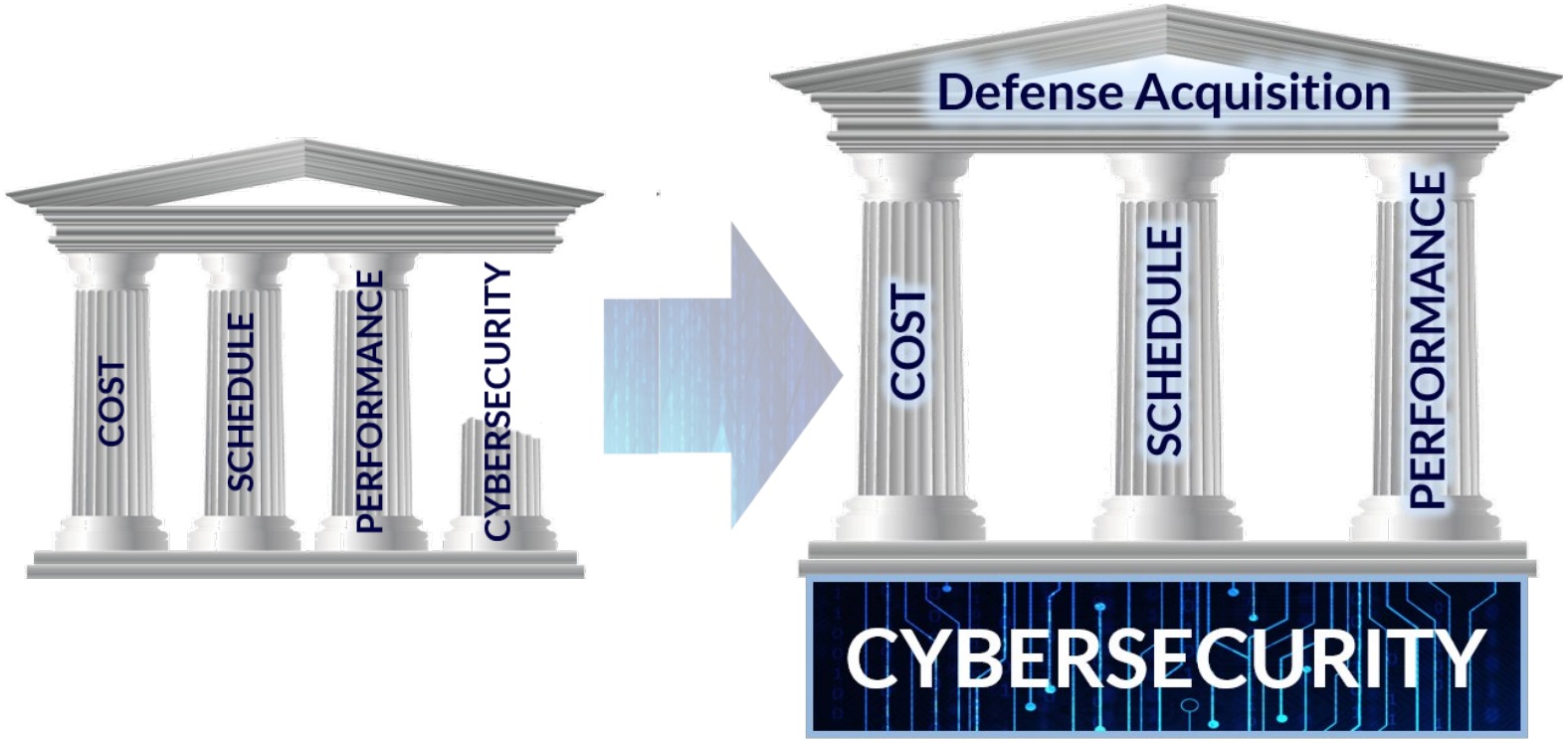
Data generated under the contract or used to manufacture goods as part of a contract.

Any CUI present in an organization will automatically qualify that organization to be Level 2 or Level 3.

Who Deals with CUI?

- Department of Defense
- NASA
- Department of Energy
- US Dept of Agriculture
- Homeland Security
- Administration
- US Dept of Commerce
- Department of Treasury
- Protection Agency
- Department of Education (Federal Student Aid)
- Nuclear Regulatory Commission
- Department of Housing and Urban Development
- Energy Regulatory Commission

Office of the Undersecretary of Defense (OUSD) for Acquisition and Sustainment (A&S)

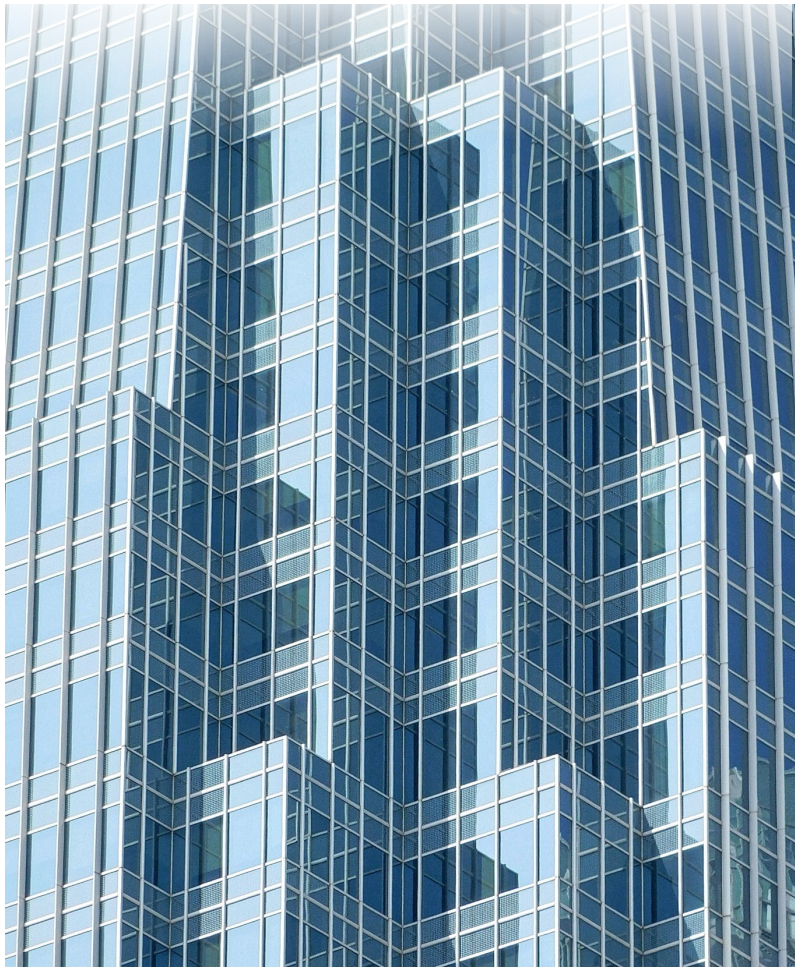


Cost, schedule, and performance are only effective in a secure environment

DFARS Clause 252.204-7012; Safeguarding Covered Defense Information and Cyber Incident Reporting

What is it?

Amended in 2016 to provide for safeguarding of CUI when being stored, processed, or transmitted through a contractor's internal information system or network



Requirements

Implement the controls within NIST SP 800-171 by December 31, 2017

Safeguard covered defense information

Report cyber incidents within 72 hours of discovery

Submit malicious software

Facilitate damage assessment

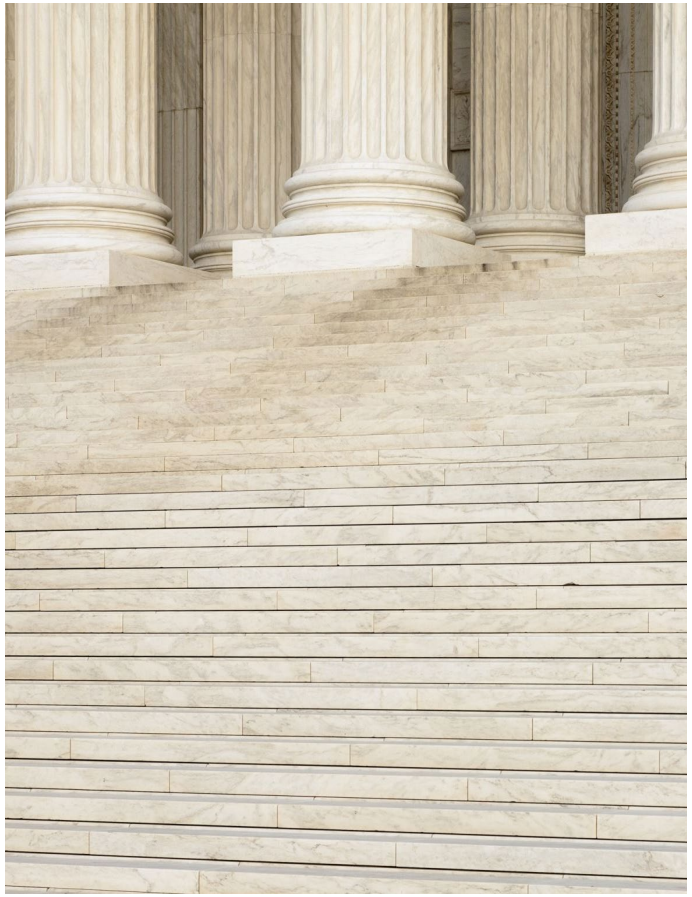
EDWARDS PERFORMANCE SOLUTIONS

DFARS 252.204-7021 | CMMC 2.0 (Nov 2021)

DFARS 252.204-7019, 7020, 7021
Cybersecurity Maturity Model Certification Requirements

- Requires ***subcontractors*** who handle, store or process sensitive data to attain their own CMMC certificate at the level appropriate for the information being flowed down to the subcontractor.

- Levels?
  - 1 = basic (FCI)
  - 2 = sensitive (CUI)
  - 3 = critical (CUI)



- Level 1 = 17 controls based on FAR Clause 52.204-21 with a **self attestation annually**
- Level 2 = 110 controls based on NIST 800-171 with a **self attestation annually** or a 3rd party assessment
- Level 3 = 20+ controls based on NIST 800-172 with a 3rd party assessment then government agency assessment
- Many contracts will have clause starting in Q3 2023

VAILLANCE GROUP
WB WARD & BERRY
EDWARDS PERFORMANCE SOLUTIONS

Self-Attestation -> Calibration

DFARS 252.204-7021 – Self-Assessment

Self- Attestation is a ***liability,*** not a celebration.

<u>False Claims Act</u> - The only way for DoD to ensure compliance

- 30% of penalty awarded to whistleblowers

CMMC and Whistleblowers

- Whistle blowers have technical expertise to help DoD /DOJ understand the impact & present solid evidence of misconduct
- Statements of Deputy Attorney General hold accountable entities that knowingly misrepresent cybersecurity activities or protocols
- Many companies providing goods & services to the DoD are not cybersecurity savvy, but lack of understanding is not an excuse

CMMC and Insider Threat

The CMMC "Awareness and Training (AT)" domain contains **AT.L2-3.2.3 Insider Threat Awareness**, which calls for an organization to "Provide security awareness training on recognizing and reporting potential indicators of Insider Threat."

The Assessment Objectives according to NIST SP 800-171A are as follows:

Determine if:

[a] potential indicators associated with insider threats are identified; and

[b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees

…"Organizations may consider tailoring insider threat awareness topics to the role (e.g. Training for managers may be focused on specific change in behavior of team members, while training for employees may be focused on more general observations."

Whistleblower vs Insider Threat

Trust

FALSE CLAIMS ACT (FCA) OVERVIEW

- History
- Prohibitions
- Damages / Civil Penalties
- Qui Tam Provisions
  - Relators
  - Intervention
  - Recovery

FCA CYBERSECURITY CASES

- *United States ex rel. Glenn v. Cisco Systems, Inc.*, No. 1:11-cv-00400-RJA (W.D.N.Y.).
  - Case settled in July 2019 with Cisco paying $8.6 million to resolve FCA allegations that it knowingly peddled flawed video surveillance gear to government agencies.
- *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245 (E.D. Cal.).
  - Case settled for a confidential amount during jury trial on April 27, 2022. Relator had argued that damages amounted to a multiple of the entire value of the contracts at issue, or $19 billion.

CIVIL CYBER-FRAUD INITIATIVE

- "The Civil Cyber-Fraud Initiative will **utilize the False Claims Act to pursue cybersecurity related fraud** by government contractors and grant recipients."
- The Civil Cyber-Fraud Initiative "will hold accountable entities or individuals that put U.S. information or systems at risk by **knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches**."

41 USC 4712 WHISTLEBLOWER PROTECTION

- Protects disclosures to employer or the government concerning:
  - Violation of law, rule, or regulation related to a federal contract
  - Gross mismanagement of a federal contract or grant
  - Gross waste of federal funds
  - Abuse of authority relating to a federal contract or grant
  - Substantial and specific danger to public health or safety
- Potential relief: reinstatement, compensatory damages (including back pay), attorneys fees
- Legal standard: "contributing factor in the personnel action"

Why Recruit a Whistleblower?

- Who?
  - Private Intelligence firms
  - Law firms
- Why?
  - Need someone with right access
  - They may need to create a whistleblower
  - Whoever brought evidence can be awarded up to 30% of fines collected
- How?
  - Outline all laws broken
  - Compile all the evidence
  - Handle the whistleblower
  - Deliver to right people to get case moving

How Do You Recruit a Whistleblower?

Spot

Assess

Develop

Recruit

Terminate

The Critical Pathway

*Shaw, E. And Sellers, L. (2015); Carnegie Mellon University

Psychology of a Deliberate Actor

Sense of MISSION (whistleblowing)

Sense of LOSS

Sense of POWER

Sense of REVENGE

Desire of RECOGNITION

Sense of CONTROL

STARTS WITH A

PERSONAL GRIEVANCE

Sense of INJUSTICE

Sense of DESTINY

Whistleblower vs Insider Threat

Trust

Applying What You Learned Today

- Next week you should:
  - Set up internal committee/task force first meeting
- In the first three months you should:
  - Determine which Federal contracts have cybersecurity obligations
  - Implement robust company-wide messaging regarding whistleblower protection
  - Conduct company-wide Insider Threat Risk Assessment
- Within six months you should:
  - Conduct a corporate compliance program assessment / gap analysis
  - Implement Insider Threat Training with accompanying confidential and anonymous reporting system; applies to leadership, all staff and external parties/vendors
  - Implement Employment Lifecycle Management (onboarding > ongoing training > offboarding) as part of Insider Threat Program