Huntington Ingalls Industries

Managing Compliance Risks and Implementation:
DFARS Cybersecurity

Introductions

Britta Brown
Manager, Compliance Program
Newport News Shipbuilding

Todd Thompson
Manager, Risk and Compliance
Ingalls Shipbuilding

Todays Topics

- Managing Compliance Risks
- Overview of the DFARS Cybersecurity Requirements
- Example: Managing the Risk and Implementation of DFARS Cybersecurity Requirements
  - Ensuring what needs to be done, gets done
  - Compliance Management Assessment Systems
    - Tool to help manage compliance risk

Disclaimer

The content discussed in this presentation is provided for informational purposes only and does not constitute legal advice or counsel. For legal advice or counsel related to issues discussed herein, please consult your attorney.

Managing Compliance Risk

Cybersecurity Key Points

Unclassified systems owned or operated by, or for, a contractor and that processes, stores or transmits “Covered Defense Information” must (at a minimum) comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171

- Deadline to “implement” NIST SP 800-171 ***was*** 12/31/2017

Areas of non-compliance must be reported to DoD CIO

- 252.204-7012(b)(2)(ii)(A)

Cyber incidents must be reported within 72 hours to:

- DoD at http://dibnet.dod.mil
- Prime Contractor (or your next higher tier contractor)

Required inclusion in all DoD contracts

Mandatory flow down to all Subcontractor Tiers

Covered Defense Information

Cybersecurity Implementation

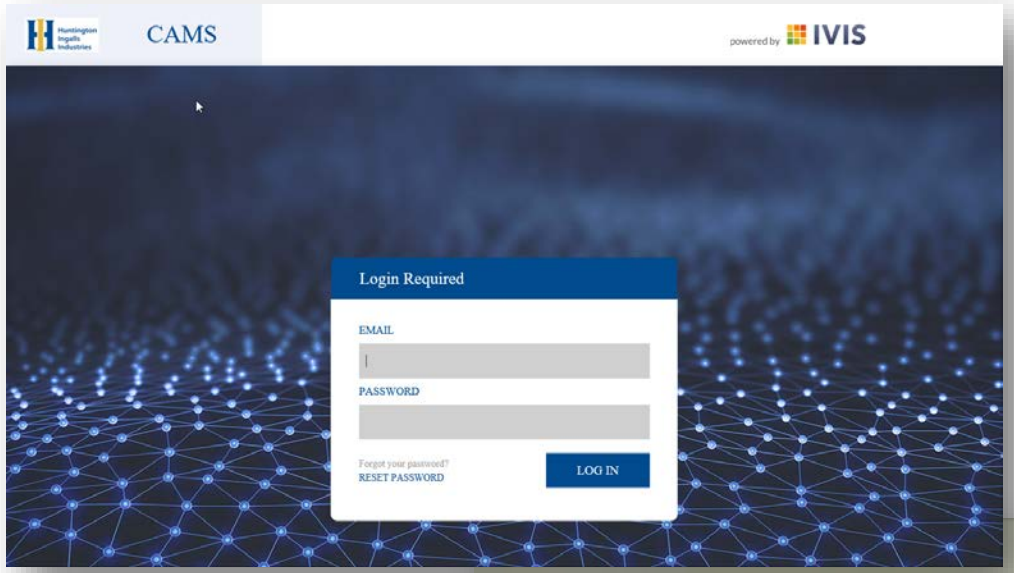
"Implementation" means:

- Having a
  - *System Security Plan (SSP)* and a
  - *Plan of Action and Milestones (POAM)*

  that accurately reflect the status of a contractor's compliance with NIST controls, even if the SSP & POAM extend beyond the December deadline.
    - NIST SP 800-171, Revision 1, dated December 2016, updated November 28, 2017

Implementation Example

- Use HII Compliance Assessment Management System as an example
  - Compliance Plan
  - Risk Assessment
  - Risk Mitigation
  - Training
  - Controls
  - Evaluation
  - SSP



Questions and Closing

- Q and A
- Thank you for attending
  - This presentation can be found on the HII Supplier webpage at http://supplier.huntingtoningalls.com/sourcing/Webinars.html
  - Questions regarding the software used at HII for managing cybersecurity implementation or any compliance area can be directed to the following:
    - Britta Brown – Britta.brown-zambrana@hii-nns.com 757-688-2786
    - Todd Thompson – MT.Thompson@hii-ingalls.com 228-935-1703

Other links

- https://www.nist.gov/sites/default/files/documents/2017/12/01/faqs.pdf Helpful facts for small manufacturers