DLA Land and Maritime

Cyber Security

Safeguarding Covered Defense Information

30-31 August 2016

NATO: 'New Realities' Make Internet a Potential Front Line in Conflict

"Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of allied operations."

Goal

Improve DLA's business relationships with vendor base to better accomplish our shared mission of supporting warfighters worldwide by mitigating risk and reducing vulnerability to cybercrime.

How

- **Provide Vendor's Updates to Cybersecurity Requirements**
  - *Define what is "Cover Defense Information"*
  - *Where and how to apply "Adequate Security"*
  - *Cyber incident reporting requirements*

Covered Defense Information (CDI)

Unclassified Information

- **Associated to Performance of Contract**
- **Provided to Contractor by or on Behalf of DoD**
- **Collected, Developed, Received, Transmitted, Used, or Stored by or on Behalf of Contractor AND:**
  - *Controlled technical information*
  - *Critical information (OPSEC)*
  - *Export Control*
  - *Information identified in the contract, that requires safeguarding or dissemination controls*

Who is Affected

- **DFARS 252.204-7012 Requires Flow Down to:**
  - *Subcontractors at all Tiers*
  - *Suppliers at all Tiers Including:*
    - Commercial suppliers
    - Commercial-off-the-shelf-item suppliers

CDI: Controlled Technical Information

- **Defined in DFARS 252.227-7013**
- **Examples:**
  - *Research and engineering data*
  - *Engineering drawings, and associated lists*
  - *Purchase Item Description (PID)*
  - *Catalog-item identification*
    - NSN with Demilitarization Code Other than “A”

CDI: Critical Information (OPSEC)

- **Specific Facts Identified through OPSEC Process:**
  - *Friendly intentions*
  - *Capabilities and activities*
  - *Needed by adversaries to plan and act effectively*

CDI: Export Control

Unclassified Information Concerning:

- *Certain items*
- *Commodities*
- *Technology*
- *Software*
- *Or other information…*

Whose Export Could Reasonably be Expected to Adversely Affect the United States National Security and Nonproliferation Objectives.

CDI: Information Identified in Contract

Any information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).

Applying “Adequate Security”

- **Information Sharing / Collaboration Toolbox**
- **Only to Information Systems Containing CDI**
- **Implement Security Protections on:**
  - *IT operated on behalf of Government*
  - *Not part of IT operated on behalf of Government*
- **On Contractors Assessed Risk or Vulnerability**

Information Sharing / Collaboration

- **Defense Industrial Base Collaboration Information Sharing Environment (DCISE)**
- **Information Sharing and Analysis Organizations (IASOs)**
- **Information Sharing and Analysis Centers (ISACs):**
  - *Defense Industrial Base ISAC*
  - *Maritime Security ISAC*
  - *Supply Chain ISAC*
  - *Surface Transportation ISAC*
  - *Cyber Information Sharing and Collaboration Program*
- FBI Infragard
- **DHS Cyber Security Evaluation Tool / NSA GRASSMARLIN**
- **Local Colleges/Universities, SANS, (ISC)², etc.**

IT Operated on Behalf of DoD

- **Cloud Computing Services**
  - *Security requirements specified in DFAR 252.239-7010*
  - *Security requirements specified in contract*

IT Not Operated on Behalf of DoD

- **National Institute of Standards and Technology (NIST)**
  - *NIST SP 800-171 Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*
- **Isolate CUI into Own Security Domain**
- **Limit Scope to CUI Particular System or Components**

Don't try to boil the ocean

NIST SP 800-171 Basic Security

Basic Security Requirements

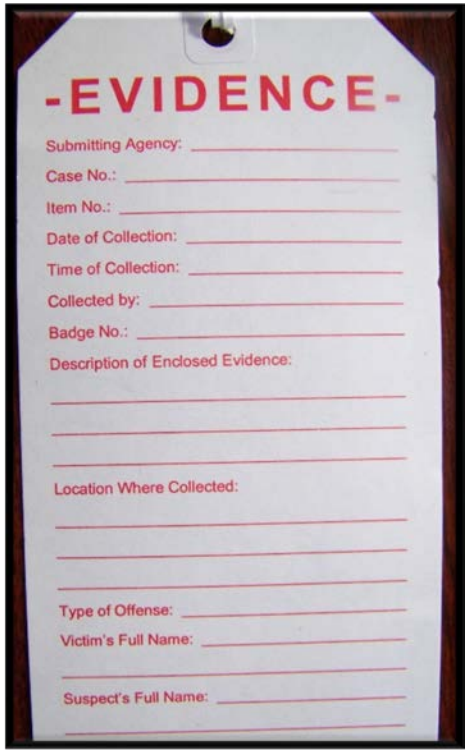
- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Information Integrity

Cyber Incident Reporting Requirements

- **Contractor Discovers a Cyber Incident Affecting:**
  - *Contractor information system*
  - *Covered Defense Information*
- **Required Elements of Cyber Incident Report**
- **DoD-approved Medium Assurance Certificate**

When You Have a Cyber Incident

- **Conduct a review for evidence of compromise of CDI**
- **Including, but not limited to:**
  - *Compromised Computers*
  - *Compromised Servers*
  - *Specific Data*
  - *User Accounts*
  - *Covered contractor information systems*



Rapidly Report to http://dibnet.dod.mil

What Goes in Cyber Incident Report

Include Elements Required by http://dibnet.dod.mil

Within 72 Hours

Within 72 Hours Report as Much of the Following

- Company name
- Company Point of Contact (POC)
- Data Universal Numbering System (DUNS) Number
- Contract number(s) or other type of agreement affected
- Contracting Officer or other agreement POC
- USG Program Manager POC
- Contract or other agreement clearance level
- Facility CAGE code
- Facility Clearance Level
- Impact to CDI
- Ability to provide operationally critical support
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- DoD programs, platforms or systems involved
- Type of compromise
- Description of technique or method used in incident
- Incident outcome
- Incident/Compromise narrative
- Any additional information

Summary

- Defined What is “Cover Defense Information”
- More Knowledgeable on “Adequate Security”
- More Knowledgeable on Cyber Incident Reporting Requirements

Have We Achieved Our Goal?

Improve DLA's business relationships with vendor base to better accomplish our shared mission of supporting warfighters worldwide by mitigating risk and reducing vulnerability to cybercrime.


Q&A


Warfighter First
People & Culture
The DLA
Land and Maritime
...Expect the Best...
Way
Process Excellence
Strategic Engagement
WARFIGHTER LOGISTICS EXCELLENCE
ACCOUNTABILITY • TEAMWORK
URGENCY • AGILITY • INNOVATION
COMMITMENT • INTEGRITY • DIVERSITY
MUTUAL TRUST & RESPECT
Financial Stewardship