DEFENSE LOGISTICS AGENCY

THE NATION' S COMBAT LOGISTICS SUPPORT AGENCY

Safeguarding Covered Defense Information within the Supply Chain

Brian Pippert, DLA J6 Cyber Resiliency

June 19-20, 2018

Did You Know

DoD manages about 4.9 million secondary inventory items, such as spare parts, with a reported value of $91.7 billion as of September 2015.

government supply chains are the most damaging threats to critical IP and systems that can adversely impact government missions

"…25 years ago, 70 percent of the goods and services the department procured were developed and produced exclusively for the military. Today, that ratio has reversed. Seventy percent of our goods and services are now either produced for commercial consumption or with commercial applications in mind. And it's backed by a largely commercial-based supply chain."

…59 percent of small and medium businesses interviewed don't have a contingency plan in place for reporting and responding to breaches. And, the U.S. Small Business Administration reported for FY2017 the DoD targeted small businesses as 34 percent of the overall subcontractor awards goal.

"… challenges for DOD today is that it does not have the level of control and visibility over its suppliers as it once did.

According to estimates by the SANS Institute up to 80 percent of all cyber breaches may have originated in the supply chain.

Rapidly expanding network of suppliers for weapons and components. For example, Northrup Grumman alone has some 5,000 suppliers in just one sector of its business.

NSA's Operation PURPLE DRAGON

(1966-67)

Proved to be one of the most effective operations ever put together by the U.S. Military

- Review its security posture from the vantage point of the enemy.
- Discovered that unclassified information released **without consideration of its sensitivity** could be used to piece together an overall picture of strategic movements and operations using:
  - Newspaper sources
  - Word of mouth
  - **Unencrypted communications**
  - **Supply shipment information**

- The team saw how an enemy force can utilize mundane information to form a hypothesis of where U.S. Forces would attack next.
- Unsecured information regarding operations was scaled back so that valuable and exploitable information could no longer flow as easily to the enemy.

Goal

Improve DLA's business relationships with vendor base to better accomplish our shared mission of supporting warfighters worldwide by safeguarding valuable and exploitable information.

BLUF

We need to safeguard our supply chains by reducing the risk of exploitation of Covered Defense Information and operationally critical support essential to the mobilization, deployment, or sustainment of the Armed Forces.

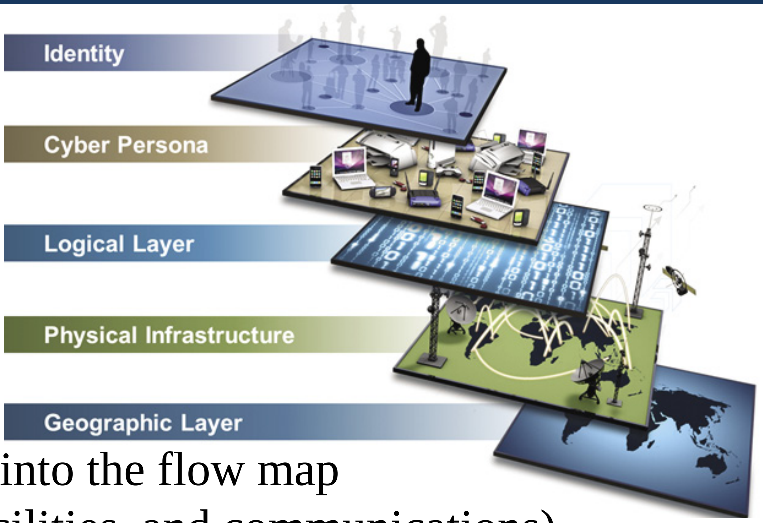
- Unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies.
- Supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

How

- Identify and Prioritize Critical Missions, Functions, and Supporting Assets
- Develop and implement a strategy to provide adequate security
- Plan for the cyber incident

Step 1: Identify and Analyze

- Mission / Business Impact Analysis
  - Single points of failure
  - Impact of delayed recovery
  - Process alternatives/work-around solutions



- Mission / Business Process Analysis
  - Key mission/business processes
  - Insert internal and external interdependencies into the flow map
  - Four pillars of continuity (leadership, staff, facilities, and communications)
  - Necessary resources (infrastructure, physical and cyber assets)
  - External interdependencies
    - Supply Chain
    - Critical service providers
    - Utilities
    - Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA) controlled resources
  - Internal interdependencies
    - Identify capabilities that could be impacted by a cyber event

98% percent of the electric power used by DoD comes from commercial providers

Due Out

Enhance existing DoD mission analysis and decomposition processes to enable a more complete identification of critical:

- ✓Capabilities
- ✓People
- ✓Geographic Locations
- ✓Physical Infrastructure
- ✓Information
- ✓Information systems assets and capabilities

subject to and outside of DoD control.

Step 2: Develop and Implement

Develop and implement a strategy to provide adequate security to Covered Defense Information and operationally critical support essential to the mobilization, deployment, or sustainment of the Armed Forces.

- Protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Analysis
Design
Development
Implementation
Evaluation

Resources and Collaboration

- Resource: DLA Website (www.dla.mil)
  - Doing Business with DLA
    - Federal Contracting Resources
      - Contractor Cyber Resources
- Collaboration:
  - Cyber Information Sharing and Collaboration Program (CISCP)
  - DoD Cyber Crime Center's DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)
  - Information Sharing and Analysis Centers (ISACs)
  - Information Sharing and Analysis Organizations (ISAOs)
  - FBI INFRAGARD

DFARS Information

- 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- Webinar: What is NIST SP 800-171 and how does it apply to small business?
- Controlled Unclassified Information (CUI) Registry
- NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- (Draft) NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations

NIST

National Institute of Standards and Technology

Training

- Center for Development of Security Excellence (CDSE)
- DHS Cyber Security Evaluation Tool / NSA GRASSMARLIN
- Federal Communications Commission’s Cyberplanner
- Information Assurance Support Environment Online Training
- National Initiative for Cybersecurity Education (NICE)
- Small Business Community (SBC) Computer Security Workshops
- U.S. Computer Emergency Readiness Team’s Resources for Business
- U.S. Small Business Administration’s Cybersecurity for Small Businesses

Requirements

NIST SP 800-171 families of security requirements

3.1 Access Control

3.2 Awareness and Training

3.3 Audit and Accountability

3.4 Configuration Management

3.5 Identification and Authentication

3.6 Incident response

3.7 Maintenance

3.8 Media Protection

3.9 Personnel Security

3.10 Physical Protection

3.11 Risk Assessment

3.12 Security Assessment

3.13 System and Communication Protection

3.14 System and Information Integrity

Implementation & Self-Assessment

- Implementation
  - Vast majority of the security requirements are associated to organizational policies and procedures.
- Self-Assessment
  - (Draft) NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information
  - Appendix D NIST SP 800-171 Maps security requirements to NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations security controls
    - NIST SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Monitoring

3.1 Access Control

- ✓ 3.1.12 Monitor and control remote access sessions.

3.3 Audit and Accountability

- ✓ 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.4 Configuration Management

- ✓ 3.4.9 Control and monitor user-installed software.

3.10 Physical Protection

- ✓ 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.
- ✓ 3.10.3 Escort visitors and monitor visitor activity.

Monitoring (cont.)

3.12 Security Assessment

- ✓ 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.13 System and Communication Protection

- ✓ 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
- ✓ 3.13.13 Control and monitor the use of mobile code.
- ✓ 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.14 System and Information Integrity

- ✓ 3.14.3 Monitor system security alerts and advisories and take action in response.

Plan for the Cyber Incident

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

- To apply to the DIB CS Program, a DoD-approved Medium Assurance Certificate is required.
- Be prepared to report within 72 hours 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

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

- Report to DoD Cyber Crime Center (https://dibnet.dod.mil/portal/intranet/)

3.6.3 Test the organizational incident response capability.

Incident Investigation

What happens after incident is reported to DCISE?

- Affected Contracting Officers are notified, and receive a copy of the report
- Contracting Officers notifies affected Requiring Activity (RA)
- RA inform chain of command, and the resulting damage assessment
- RA coordinates with the Damage Assessment Management Office (DAMO), and decides within 90 days if a request will be made for Contractor media/data and provides rationale.
  - RA and Contracting Officer submit request to DCISE
  - DCISE requests and receives comprised media
  - DCISE transfers media to DAMO
  - DAMO conducts DFARS cyber incident damage assessment.
  - DAMO distributes classified and unclassified reports as required.

- Requiring Activity assess and implement appropriate programmatic, technical, and/or operational actions to mitigate risks identified in the damage assessment report.

Summary

We need to secure our supply chains by reducing the risk of exploitation of Covered Defense Information and/or operationally critical support essential to the mobilization, deployment, or sustainment of the Armed Forces. This can be accomplished by:

- Identifying and Prioritizing Critical Missions, Functions, and Supporting Assets
- Develop and implement a strategy to provide adequate security
- Plan for the inevitable cyber incident involving Covered Defense Information and/or operationally critical support essential to the mobilization, deployment, or sustainment of the Armed Forces.

Questions

Safeguarding Covered Defense Information within the Supply Chain