DEFENSE LOGISTICS AGENCY

Supply Chain Security Strategy

Strengthening Operational Resiliency

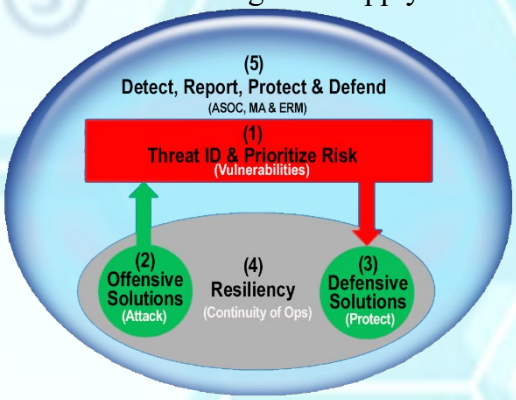
What is DLA's Supply Chain Security Strategy (SCSS)?

It is the Agency's roadmap to address supply chain security (SCS) challenges across the enterprise. The strategy is designed to establish an enterprise architecture that does these 5 things:

- Identifies and report threats, vulnerabilities and prioritizes risk
- Develops risk-mitigating offensive solutions to minimize threats
- Develops risk-mitigating defensive solutions to protect vulnerabilities
- Infuses resiliency into systems, processes, infrastructure and people
- Prevents disruption through detection, protection, reporting and defense of the global supply chain

How Will DLA Achieve This Strategy?

To develop that architecture, DLA will concentrate on four **Strategic Focus Areas**. Strategic Focus Areas are "strategy bins" that house supply chain security-related initiatives (diamond bullets below) that are mapped to objectives in the Agency's Strategic Plan. The initiatives put the strategy in motion by actuating the Strategic Focus Areas for the purpose of developing the architecture.



Strategic Focus Area #1: Institutionalize Supply Chain Security

- **Integrate SCS into Mission Assurance (MA) Portfolio**
  - Develop comprehensive vulnerability assessments
  - Integrate SCS into Enterprise Risk Management
- **Integrate Ops Scorecard Into Dashboard**
  - **Phase I** – Develop concept, prototype and process
  - **Phase II** – Identify existing data feeds & thresholds
  - **Phase III** – Finalize J6 design requirement & integrate

Strategic Focus Area #2: Maintain Integrity and Access to Key Data

- **Operationalize Cybersecurity Strategy**
  - Define and defend mission relevant & key cyber terrain
  - Reduce cyber risk by eliminating Data Centers
  - Reduce cyber risk by replacing aging servers/routers
- **Establish Cybersecurity as Award Discriminator**
  - Identify critical contract cyber evaluation factors
  - Leverage DARPA Log-X for vendor cyber-assurance
- **Strengthen Technical Data Controls**
  - Implement enhanced supplier validation for data export
  - Develop capability to block foreign IP addresses
  - Minimize time Technical Data Packages (TDPs) are made available in DLA's repository

Strategic Focus Area #3: Partner With Reputable Vendors

- **Prevent Counterfeit & Non-Conforming Parts**
  - Continue "DNA-Marking" for microelectronics
  - Integrate Business Decision Analytics and Vendor Network Mapping into acquisition strategies
  - Collaborate with Trade & Distribution Fraud councils and Procurement Working Groups
  - Enhance DIBBS to mitigate risk from distributors
- **Enhance Knowledge of Supply Chain Risk Management Tools for Acquisition Workforce**
  - Identify tools, requirements and deploy training
- **Improve Market Intelligence (MI) Capabilities**
  - Develop MI business processes & procedures
  - Conduct Research and Development pilots

Strategic Focus Area #4: Strengthen Resiliency

- **Improve Mission Resiliency; *People, Technology and Infrastructure***
  - Exploit tech to optimize risk ID, analysis & reporting
  - Develop Supply Chain Security education campaign
- **Reduce Cyber Risk to Installation & Control Systems**
  - Develop mitigation program for critical control systems
- **Establish Counterintelligence (CI) Support Plans**
  - Conduct CI assessments & prioritize Supply Chain risk
  - Implement CI support plans for Supply Chain assets