DEFENSE LOGISTICS AGENCY

The Nation's Combat Logistics Support Agency

SUPPLY CHAIN SECURITY STRATEGY

Strengthening Operational Resiliency

Appendix 1 to DLA's 2018 - 2026 Strategic Plan

DEFENSE LOGISTICS AGENCY
MESSAGE FROM THE DIRECTOR

DLA's Supply Chain Security Strategy is the roadmap for how the Agency will address supply chain security challenges across the enterprise. This cross-cutting effort is fundamental to our operations and underpins DLA's ability to support the Warfighter. Interruption of DLA supply chain operations compromises our nation's ability to deliver combat power and execute critical missions. It's that serious!

As the nation's Combat Logistics Support Agency responsible for end-to-end management of nine supply chains supporting the Warfighter, DLA has an inherent imperative to ensure we have the proper detection, protection, redundancy and resilience built into our systems, processes, infrastructure and people to ensure continued support to the Warfighter.

Today's world presents a multitude of challenges to DLA's supply chain operations. Threats from natural disasters, geopolitical developments, nefarious activities, diminishing manufacturers, and the ever-present threat from the cyber-domain demand that DLA continues the journey to strengthen operational resiliency. As the threat environment evolves, so too must DLA's ability to detect, protect, and continue operations in a contested or degraded environment through redundant and resilient supply chain operations.

This document carves a path forward for the Agency to follow in pursuit of strengthening operational resiliency across the enterprise. The strategy within it anchors to the fundamental elements of Supply Chain Risk Management (SCRM) and Mission Assurance. I need every DLA member to understand this strategy and to support it wherever you may fit in because supply chain disruption is not an option for the Warfighter. With each of us synchronized on supply chain security, together we can thwart disruption by strengthening operational resiliency.

Darrell K. Williams
Lieutenant General, US Army
Director, Defense Logistics Agency

Warfighter First!

TABLE OF CONTENTS

Warfighter First!

STRATEGIC CONTEXT

DELIVER UNCOMPROMISED

> **"Today our adversaries may have a better understanding of our strategic vulnerabilities than do we. This includes vulnerabilities introduced via networks or through the supply chain. This is because of poor/inadequate intelligence on such threats, excessive compartmentation that precludes effective sharing of such threat information, lack of prioritization, and widespread availability of information in the public domain."**
>
> *- MITRE Report, 8 Aug 2018, Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*

DLA'S GLOBAL SUPPLY CHAIN

While speaking at the HQ CIA Supply Chain Summit in April 2019, the Joint Staff Director for Logistics observed that the character of logistics has changed dramatically over the years, but the nature of logistics remains the same. Getting the right things where they need to be at the right time and in serviceable condition has always been the primary objective. However, in the current technology-enabled environment, "the way" logisticians accomplish that is very different compared to the past. Today's supply chains are expansive, non-linear, and highly relationship-dependent. DLA's Global Supply Chain is staggeringly expansive and consists of Acquisitions, Storage, Distribution, and Disposal primary mission-sets. It extends to 46 states and 28 countries and encompasses a myriad of complex and interconnected systems, processes, facilities, infrastructure, suppliers, transportation nodes, end-users, and employees. Twenty-three sub-elements enable these primary components of DLA's Global Supply Chain. They include business processes, business systems, distribution centers, vendor-networks, industrial support, financial health, employee readiness, cybersecurity, DLA's six Major Subordinate Commands and nine supporting supply chains. Each of these supply chain components and sub-elements are susceptible to adversarial exploitation and disruption from a host of potential threats.

SUPPLY CHAIN SECURITY VS. SCRM

Supply Chain Security is DLA's ***comprehensive approach to protect supply chains,*** key infrastructure and critical assets in order to assure uninterrupted delivery of proactive global logistics in peace and war.

Supply Chain Risk Management (SCRM) is the ***process for managing risk*** by identifying, assessing and mitigating threats, vulnerabilities and disruptions to the DOD supply chain from beginning to end to ensure mission effectiveness.

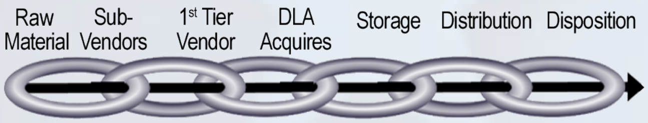
- DODI 4140.01

THREAT SPECTRUM

Cyber-attacks are a continuous threat to DLA's Global Supply Chain due to the interconnectedness of our information technology-dependent operations. There are more electronic devices than people in DLA, and cyber-attackers are growing in their sophistication. Each year there are millions of attempts to access sensitive information on the DoD network. However, the threat spectrum extends far beyond cyber-attacks. Natural and man-made disasters and accidents can disrupt a vendor's ability to supply DLA critical parts for the Warfighter for an extended period of time. Geopolitical developments have the potential to constrain DLA's access to allied partners, vendors, and critical resources. The proliferation of sensitive information by the unintentional mishandling of export controlled technical data can lead to an adversary's ability to intercept US military technology. Bad-actors engaging in nefarious activities can steal the identity of legitimate suppliers, introduce counterfeit parts into DLA's Global Supply Chain, and disrupt the Agency's financial position. Sole-source and diminishing manufacturers can ground fleets of aircraft if they choose to discontinue operations while foreign dependencies and lack of visibility into sub-tier suppliers can lead to additional counterfeiting, cyber-attack, and espionage.

DESIRED END STATE

DLA's mission is to sustain Warfighter readiness and lethality by delivering proactive global logistics in peace and war. Maintaining an effective supply chain security posture through Supply Chain Risk Management (SCRM) is fundamental to the Agency's ability to meet its mission. It is within the threat spectrum captured above that DLA must innovate to strengthen operational resiliency in support of the Warfighter. DLA must continuously identify, assess, report and mitigate threats, vulnerabilities, and disruptions to its Global Supply Chain. DLA's end state is to establish an enterprise architecture that comprehensively addresses supply chain security challenges. An architecture that evolves as new threats emerge, one that endures the test of time and provides uninterrupted support to the Warfighter.



*DLA's supply chains are diverse and complex…
and must be secured across the materiel life cycle*

DLA'S SUPPLY CHAIN SECURITY ARCHITECTURE

What does a "secure" global supply chain look like? DLA's overall supply chain security strategy is designed to establish an architecture that comprehensively addresses supply chain security from an enterprise perspective. The architecture consists of five broad components. These components are depicted in Figure 1 and explained in the following 5 paragraphs:

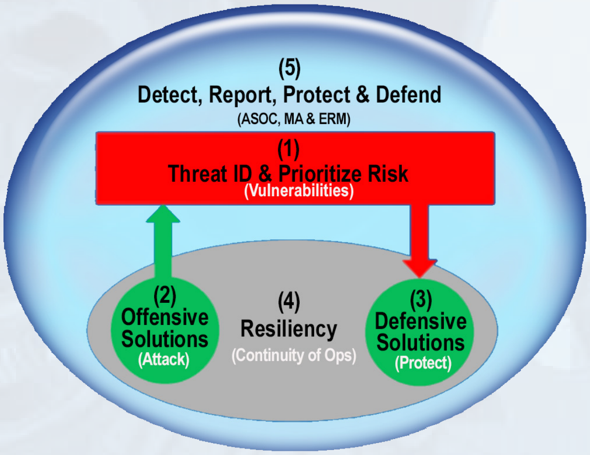


Figure 1. DLA's Supply Chain Security Architecture

THREAT/VULNERABILITY IDENTIFICATION AND RISK PRIORIZATION

The first architectural component is foundational to the Agency's supply chain security strategy. Its purpose is to establish a repeatable process to identify and report threats and vulnerabilities across DLA's expansive Global Supply Chain and to prioritize associated risk. To strengthen operational resiliency, DLA must first understand where the "soft-underbellies of logistics" are within the Agency. This first architectural component does that. The process must be comprehensive, repeatable and continuous, given the emergent and ever-changing nature of threats.

OFFENSIVE RISK-MITIGATION SOLUTIONS

The second architectural component is dependent upon the first. Once threats are identified, DLA must have the ability to develop innovative offensive mitigating solutions that attack and minimize those threats. Examples of offensive solutions include market-intelligence, cyber-operations and DNA-marking of microelectronics.

DEFENSIVE RISK-MITIGATION SOLUTIONS

Similarly, once vulnerabilities are identified, DLA must have the ability to develop innovative defensive solutions that protect vulnerabilities and mitigate risk. Examples of defensive solutions include Business Decision Analytics, Vendor Network Mapping and Export Controlled Technical Data Supplier Validation Processes.

RESILIENT SUPPLY CHAIN OPERATIONS

The fourth architectural component is the guarantor of uninterrupted support to the Warfighter. Its purpose is to infuse resiliency into DLA's systems, processes, infrastructure and people. In the event that an adversary or natural disaster threatens DLA's Global Supply Chains, resilient supply chain operations ensure the mission continues. Examples of resiliency include redundant capabilities, continuity of operation plans and systems hardening.

PREVENTION THROUGH DETECTION, PROTECTION AND DEFENSE

The purpose of the fifth architectural component is to operationalize supply chain security within the Agency and to ensure that it endures the test of time. DLA must continuously prevent disruption by integrating supply chain security into the Agency Synchronization and Operations Center business rules in order to effectively detect, report, protect and defend against emergent threats. The Agency must also fully integrate SCRM into DLA's Mission Assurance portfolio and ultimately into the Enterprise Risk Management framework to ensure that supply chain security is addressed from an enterprise perspective.

DID YOU KNOW?

DNA Marking of Microelectronics: To counter the growing sophistication of counterfeiters, DLA launched an anti-counterfeiting program to improve delivery time, reduce costs, strengthen supply chain controls and enhance quality assurance. DNA marking consists of applying a botanical DNA identifier to the surface of a microcircuit to authenticate originality. The DNA mark cannot be replicated and deters counterfeiters. A hand-held scanner for easy identification within the supply chain can detect the DNA mark. The mark can also be used for forensic testing by providing detailed information about the microcircuit, such as supplier, CAGE code, part and lot number.

Vendor Network Mapping: Relationships in DLA supply chains are complex. However, DLA is employing a powerful tool to map vendor networks from Tier 1 through Tier 3 suppliers called Vendor Network Mapping. This capability makes it possible to look upstream in vendor networks to identify risks in areas such as vendor financial position, compliance, legal and foreign relationships.

SUPPLY CHAIN SECURITY STRATEGIC FOCUS AREAS

To create an architecture that comprehensively addresses supply chain security from an enterprise perspective, DLA will concentrate on the following four Strategic Focus Areas:

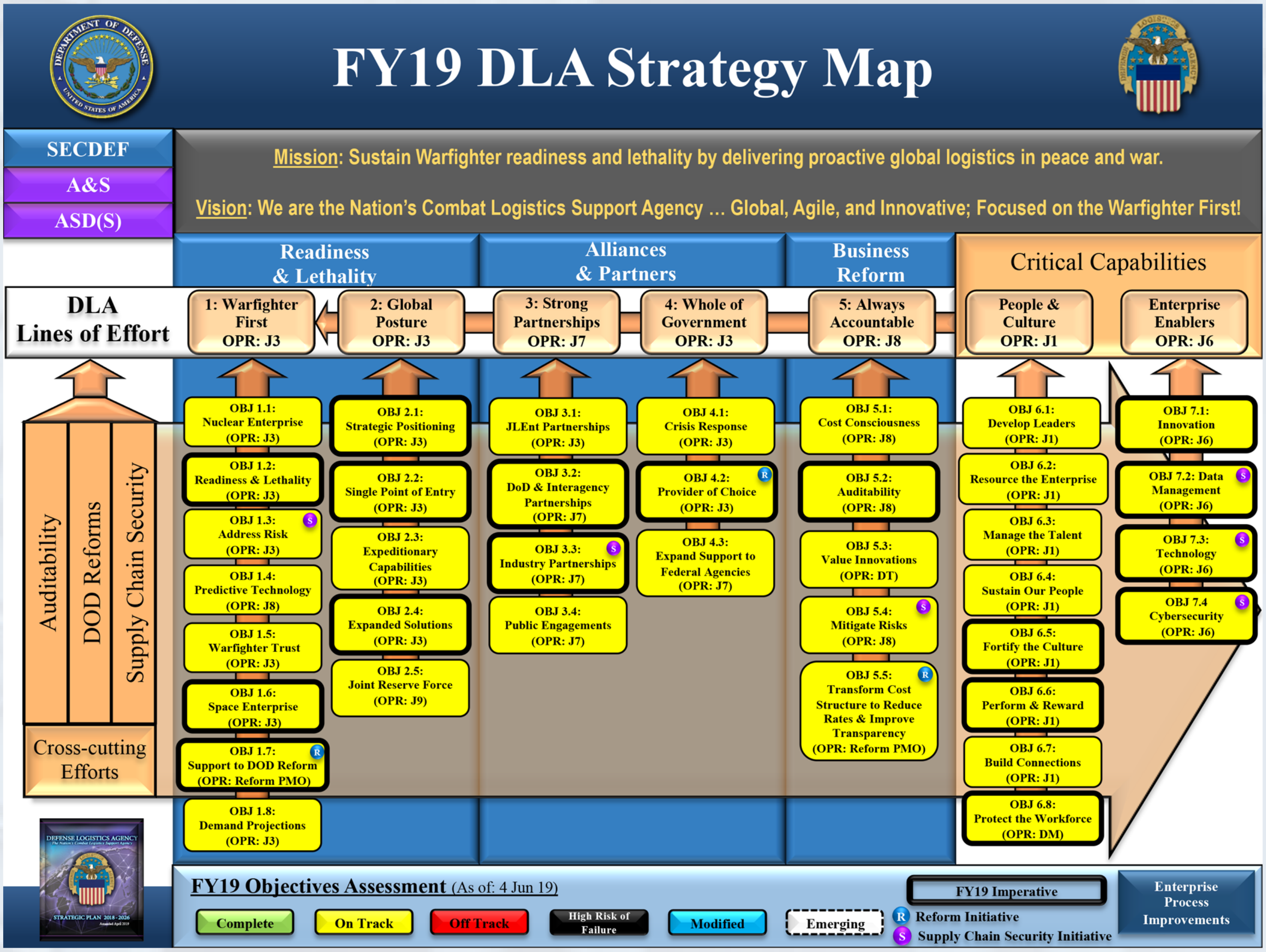
- Institutionalize Supply Chain Security across the DLA enterprise
- Maintain integrity and access to key data
- Partner with valid, reputable vendors who produce quality supplies and services
- Strengthen the resiliency of systems, processes, infrastructure and people

The Strategic Focus Areas represent "strategy bins" that house supply chain security-related initiatives, which are mapped to objectives within DLA's 2018-2026 Strategic Plan. Those objectives are depicted in Figure 2 as indicated by the purple circle labeled with an "S" (Ⓢ).

The supply chain security initiatives are the essence of DLA's overall supply chain security strategy. They put the strategy into motion by actuating the four Strategic Focus Areas for the purpose of achieving an architecture that comprehensively addresses DLA's supply chain security challenges. The next four sections takes a closer look at each of them.

INSTITUTIONALIZE SUPPLY CHAIN SECURITY ACROSS THE DLA ENTERPRISE

The first Strategic Focus Area underwrites DLA's ability to execute its Mission Essential Functions during peace and war, regardless of the nature of disruption. The bedrock initiative within this Strategic Focus Area is integrating Supply Chain Security into the Agency's Mission Assurance portfolio and Enterprise Risk Management framework. Key and essential to this is developing a standardized, repeatable process to assess enterprise-wide supply chain



FY19 DLA Strategy Map

SECDEF
A&S
ASD(S)

Mission: Sustain Warfighter readiness and lethality by delivering proactive global logistics in peace and war.

Vision: We are the Nation's Combat Logistics Support Agency … Global, Agile, and Innovative; Focused on the Warfighter First!

Readiness & Lethality
Alliances & Partners
Business Reform
Critical Capabilities

DLA Lines of Effort
1: Warfighter First OPR: J3
2: Global Posture OPR: J3
3: Strong Partnerships OPR: J7
4: Whole of Government OPR: J3
5: Always Accountable OPR: J8
People & Culture OPR: J1
Enterprise Enablers OPR: J6

Auditability
DOD Reforms
Supply Chain Security
Cross-cutting Efforts

OBJ 1.1: Nuclear Enterprise (OPR: J3)
OBJ 1.2: Readiness & Lethality (OPR: J3)
OBJ 1.3: Address Risk (OPR: J3) Ⓢ
OBJ 1.4: Predictive Technology (OPR: J8)
OBJ 1.5: Warfighter Trust (OPR: J3)
OBJ 1.6: Space Enterprise (OPR: J3)
OBJ 1.7: Support to DOD Reform (OPR: Reform PMO) Ⓡ
OBJ 1.8: Demand Projections (OPR: J3)

OBJ 2.1: Strategic Positioning (OPR: J3)
OBJ 2.2: Single Point of Entry (OPR: J3)
OBJ 2.3: Expeditionary Capabilities (OPR: J3)
OBJ 2.4: Expanded Solutions (OPR: J3)
OBJ 2.5: Joint Reserve Force (OPR: J9)

OBJ 3.1: JLEnt Partnerships (OPR: J3)
OBJ 3.2: DoD & Interagency Partnerships (OPR: J7)
OBJ 3.3: Industry Partnerships (OPR: J7) Ⓢ
OBJ 3.4: Public Engagements (OPR: J7)

OBJ 4.1: Crisis Response (OPR: J3)
OBJ 4.2: Provider of Choice (OPR: J3) Ⓡ
OBJ 4.3: Expand Support to Federal Agencies (OPR: J7)

OBJ 5.1: Cost Consciousness (OPR: J8)
OBJ 5.2: Auditability (OPR: J8)
OBJ 5.3: Value Innovations (OPR: DT)
OBJ 5.4: Mitigate Risks (OPR: J8) Ⓢ
OBJ 5.5: Transform Cost Structure to Reduce Rates & Improve Transparency (OPR: Reform PMO) Ⓡ

OBJ 6.1: Develop Leaders (OPR: J1)
OBJ 6.2: Resource the Enterprise (OPR: J1)
OBJ 6.3: Manage the Talent (OPR: J1)
OBJ 6.4: Sustain Our People (OPR: J1)
OBJ 6.5: Fortify the Culture (OPR: J1)
OBJ 6.6: Perform & Reward (OPR: J1)
OBJ 6.7: Build Connections (OPR: J1)
OBJ 6.8: Protect the Workforce (OPR: DM)

OBJ 7.1: Innovation (OPR: J6)
OBJ 7.2: Data Management (OPR: J6) Ⓢ
OBJ 7.3: Technology (OPR: J6) Ⓢ
OBJ 7.4 Cybersecurity (OPR: J6) Ⓢ

FY19 Objectives Assessment (As of: 4 Jun 19)
Complete
On Track
Off Track
High Risk of Failure
Modified
Emerging
FY19 Imperative
Ⓡ Reform Initiative
Ⓢ Supply Chain Security Initiative
Enterprise Process Improvements

Figure 2. FY19 DLA Strategy Map

vulnerabilities. Establishing such a process is foundational to DLA's ability to identify and report vulnerabilities and to prioritize, manage and mitigate supply chain risk. This initiative also unequivocally assigns the Office of Primary Responsibility for Supply Chain Security to DLA J3, Logistics Operations. Explicit ownership of this cross-cutting effort enables an integrated approach to securing DLA's Global Supply Chain.

This Strategic Focus Area also includes an initiative to finalize the development of the Agency's Resilient Supply Chain Operations Scorecard which will provide a "live" operational view of DLA's Supply Chain Security environment. The Scorecard includes DLA's primary supply chain components and 23 sub-elements and portrays them from an Agency, Major Subordinate Command and Regional Command perspective. This live-fed resource will be integrated into DLA's Enterprise Dashboard which will allow the Agency Synchronization and Operations Center to proactively prevent supply chain disruption through detection, protection and defense of DLA's Global Supply Chain. The initiative takes a phased approach to implementation by first (Phase I) developing the initial concept and business rules for its use. Phase II then incorporates existing feeds within the Enterprise Dashboard for an initial live-view and Phase III maps the remaining feeds and fully integrates the completed Scorecard into the Enterprise Dashboard.

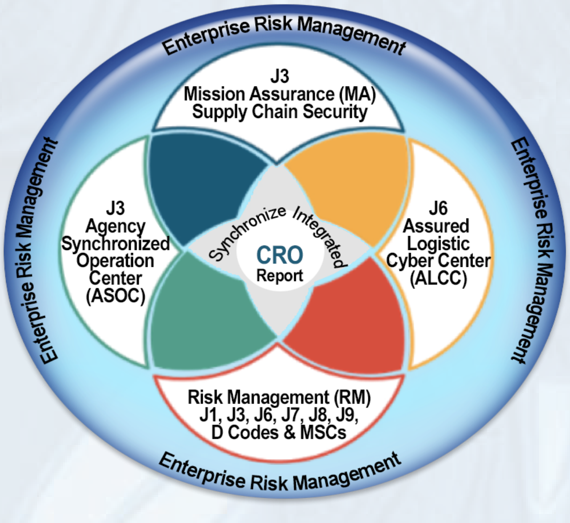


Figure 3. Enterprise Risk Management

MAINTAIN INTEGRITY AND ACCESS TO KEY DATA

The second Strategic Focus Area includes two primary initiatives that protect data and network systems. The first one is designed to protect the Agency's data and systems for internal use by operationalizing DLA's Cybersecurity Strategy. Data and system breaches can cause significant disruption to supply chain operations. They are often times more difficult to detect and counter and can undermine confidence in the data or system in ways other disruptions do not. This initiative operationalizes DLA's deployment of layered cybersecurity activities to protect, defend and infuse resiliency into information technology systems. Maintaining a secure and resilient cyberspace operating environment and ensuring prioritized remediation of top cyber risks are essential components of this initiative. It also sets in motion an effort to explore strategic partnerships between DLA and US Transportation and Cyber Commands to provide integrated, secure supply chain solutions to DoD. The Global Supply Chain is as strong as its weakest link. Because of this, strategic alignment among these partners is critical to ensure cyber-secure transitions between DLA supply chain operations and USTRANSCOM mission sets.

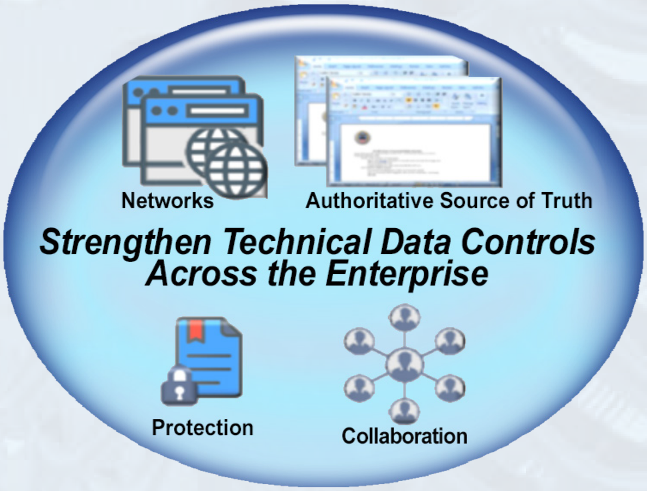

Networks
Authoritative Source of Truth
Strengthen Technical Data Controls
Across the Enterprise
Protection
Collaboration

Figure 4. Technical Data Controls

The second initiative strengthens Operations Security (OPSEC) practices by controlling the exportation of DLA's data to external partners through various measures. Much of DLA's data is sensitive in nature. Military specifications and standards, technical data packages (TDP), schematics, customer delivery destinations and many other forms of exportable data are subject to exploitation if in the wrong hands. This initiative strengthens technical data controls across the enterprise by instituting an enhanced validation procedure for suppliers requiring access to export controlled technical data and develops the capability to block foreign Internet Protocol addresses from accessing export controlled data stored in DLA's data repository. This initiative also assigns the highest level of restriction to the data repository for exportable data that includes a TDP and minimizes the amount of time a TDP is made available in the repository.

CONTINUED SUPPLY CHAIN SECURITY STRATEGIC FOCUS AREAS

A third initiative within this Strategic Focus Area optimizes the use of cybersecurity as a discriminator in source selections and awards to ensure DLA conducts business with vendors who take appropriate action to protect DoD sensitive data and information. The Agency will also continue its collaborative partnerships with academia and industry to share Supply Chain Security best practices and innovations with an emphasis on cybersecurity and data protection.

PARTNER WITH VALID, REPUTABLE VENDORS WHO PRODUCE QUALITY SUPPLIES & SERVICES

The purpose of the third Strategic Focus Area is to ensure that the vendors DLA partners with produce high-quality materiel for the Warfighter. The accompanying initiatives are heavily focused on preventing counterfeit and non-conforming parts from entering into DLA's Global Supply Chain. With well established processes in-place to ensure DLA partners with valid and reputable vendors, fraudulent exploitation still exists given the sheer volume of purchases, business transactions and the automation required to support them. Further complicating this is the complexity of sub-vendor relationships that support DLA's primary vendor base. DLA has limited insight into these relationships which often times have several upstream providers, foreign dependencies and a multitude of potential entry points for counterfeit and non-conforming parts to enter into DLA's Global Supply Chain.

To protect against counterfeit parts and fraudulent vendor activity, DLA engages in a number of mitigating activities. First, the Agency will continue to "DNA mark" trusted-source microcircuits through DLA's Product Test Center for Electronics in order to positively identify integrated circuit cards throughout their life cycle. The Agency will also refine and implement vendor network mapping tools and Business Decision Analytics platforms to help identify sub-vendor relationships and enhance DLA's ability to report suspect counterfeit activity to the Defense Criminal Investigation Service.

OPERATIONS SECURITY

Operations Security (OPSEC) is a systematic process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities. DLA must be ever vigilant when handling logistics information and must protect it at all times, especially when interacting with its vendor network. Each DLA organization maintains Critical Information and Indicators Lists that identify unclassified but sensitive information that must be protected from disclosure.

BUSINESS DECISION ANALYTICS

DLA uses a decision support tool called Business Decision Analytics (BDA) to analyze nearly 1 million bids a day to help mitigate procurement risk. BDA is part of a suite of tools that use machine learning, predictive variables, multiple data sources and advanced analytics to help make informed material and purchasing decisions by evaluating supplier, solicitation, price and item risk. BDA helps DLA mitigate risk when making material and purchasing decisions.

DLA will also continue its collaborative efforts to enhance the Agency's capabilities to protect against counterfeit parts and supplier fraud through existing cross-functional working groups. Three in particular provide tremendous opportunities for functional area experts to engage at the enterprise level to address the counterfeit/fraud problem-set; the *Technical Quality (TQ) - Distribution Fraud Council, the TQ - Trade Security Fraud Council and the Procurement Working Group*. Discovery from these working groups will be captured in a revised version of DLA Instruction 4000.04, *Counterfeit Materiel Prevention and Mitigation*. DLA is also in the process of developing enhancements to DLA's Internet Bid Board System (DIBBS) to strengthen the Agency's capabilities to mitigate counterfeit and fraud risk when procuring parts from an independent distributor as opposed to a trusted supplier within DLA's existing vendor base. DLA also established a market intelligence initiative designed to give the Agency a better understanding of the atmospherics within its vendor network. Fundamental to this initiative is the development of a business process focused on collecting, analyzing and disseminating actionable intelligence for specific markets of interest to help shape acquisition strategies.

STRENGTHEN RESILIENCY OF SYSTEMS, PROCESSES, INFRASTRUCTURE AND PEOPLE

The fourth Strategic Focus Area ensures DLA's support to the Warfighter continues even in the midst of disruptive activity. The supporting initiatives were developed to strengthen operational resiliency by building resiliency into the Agency's systems, processes, infrastructure and people. The hallmark initiative within this Strategic Focus Area is designed to make the Agency's supply chains resilient to all hazards and threats. To achieve this, DLA will enhance supply chain resiliency by continuing to provide world-class protection to its employees and

OPSEC is everyone's job!

Figure 5. Supply Chain Elements

infrastructure. These two critical supply chain resources are key and essential to successful supply chain operations. Facilities must be secure and reliable and employees must be able to detect and prevent disruptions and spring into action to provide continued operations when disruptions occur. DLA will also strengthen resiliency in its infrastructure by reducing cyber risks to installations and critical facility control systems through the development of an inventory, assessment and mitigation program for mission critical control systems.

DLA will also strengthen operational resiliency by exploiting current and emerging technologies that optimize supply chain risk identification, analysis and reporting through internal and external stakeholder collaboration. The Agency will also establish comprehensive counterintelligence support plans for critical elements of the Global Supply Chain. These tailored support plans will identify and mitigate counterintelligence vulnerabilities within specific supply chains, deter threats posed by Foreign Intelligence Entities (FIE) and preempt foreign intelligence targeting of DLA's supply chains for the purpose of strengthening operational resiliency.

WHAT'S THE DIFFERENCE?

Resiliency: Defines the ability to recover, converge or self-heal to restore normal operations after a disruptive event.

Redundancy: Idefines the deployment or provisioning of duplicate devices or systems in critical areas to take over active operation if the primary device or system fails.

Continuity of operations is a key aspect of this Strategic Focus Area and to the Agency's overall Supply Chain Security Strategy because it ensures uninterrupted support to the Warfighter during disruptive events. DLA has extensive continuity of operations plans (COOP) that underwrite the Agency's Mission Essential Functions. The plans range from broad enterprise-wide mission areas, to Major Subordinate Command/supply chain problem-sets and process/system-specific mission areas. DLA ensures continuity of operations through devolution/relocation plans and back-up processes for key systems and infrastructure through a range of resilient and redundant capabilities. DLA will continue to develop and refine its plans to guarantee continuity of operations and evaluate them through continuous tests and exercises to ensure plans are effective in providing uninterrupted support to the Warfighter.

ROLE OF COUNTERINTELLIGENCE

The mission of the DLA Counterintelligence (CI) Program Office is to neutralize and mitigate FIE attempts to exploit DLA's global supply chain as well as acquisition vulnerabilities. By leveraging organic capabilities and relationships with the intelligence community, the CI Program Office assesses CI vulnerabilities of DLA equities, analyzes corresponding FIE threats, and develops tailored CI support plans to better ensure the integrity and security of the entire DLA supply chain.

LEVERAGING ENTERPRISE ENABLERS

The 2018-2026 DLA Strategic Plan Enterprise Enablers are essential ingredients in the recipe for successful Supply Chain Security Strategy. *Innovation, Data Management, Technology and Cybersecurity* underpin the initiatives within the four Supply Chain Security Strategic Focus Areas. They leverage key attributes of each to amplify and synthesize the multitude of cross-functional tasks associated with implementing the individual initiatives.

Securing DLA's expansive Global Supply Chain, within the context of a broad threat spectrum, calls on the Agency to unlock new solutions to non-linear challenges through bold, innovative ideas. It also demands effective data management techniques to fully integrate the Resilient Supply Chain Operations Scorecard into the Enterprise Dashboard in order to provide a comprehensive, digitized view of the supply chain security landscape. It also requires the Agency to leverage readily accessible and emerging technologies to drive competitive advantage and effective supply chain solutions for the Warfighter. Technological solutions that are trusted, safe and cyber secure.

✔ INNOVATION

Design Sprints ♦ Crowdsourcing ♦ Prototyping

✔ DATA MANAGEMENT

Analytics ♦ Dashboards ♦ Digitization

✔ TECHNOLOGY

Artificial Intelligence ♦ 3D Printing ♦ Automation

✔ CYBERSECURITY

Prevention ♦ Detection ♦ Virtualization

CONCLUSION

Maintaining an effective supply chain security posture is key and essential to DLA's ability to support the Warfighter. The Agency's Supply Chain Security Strategy is designed to establish an enterprise architecture that comprehensively addresses supply chain security challenges. An architecture that evolves as new threats emerge, one that endures the test of time and provides uninterrupted support to the Warfighter. The four Strategic Focus Areas, actuated by their associated supply chain security initiatives, were developed to create that architecture.

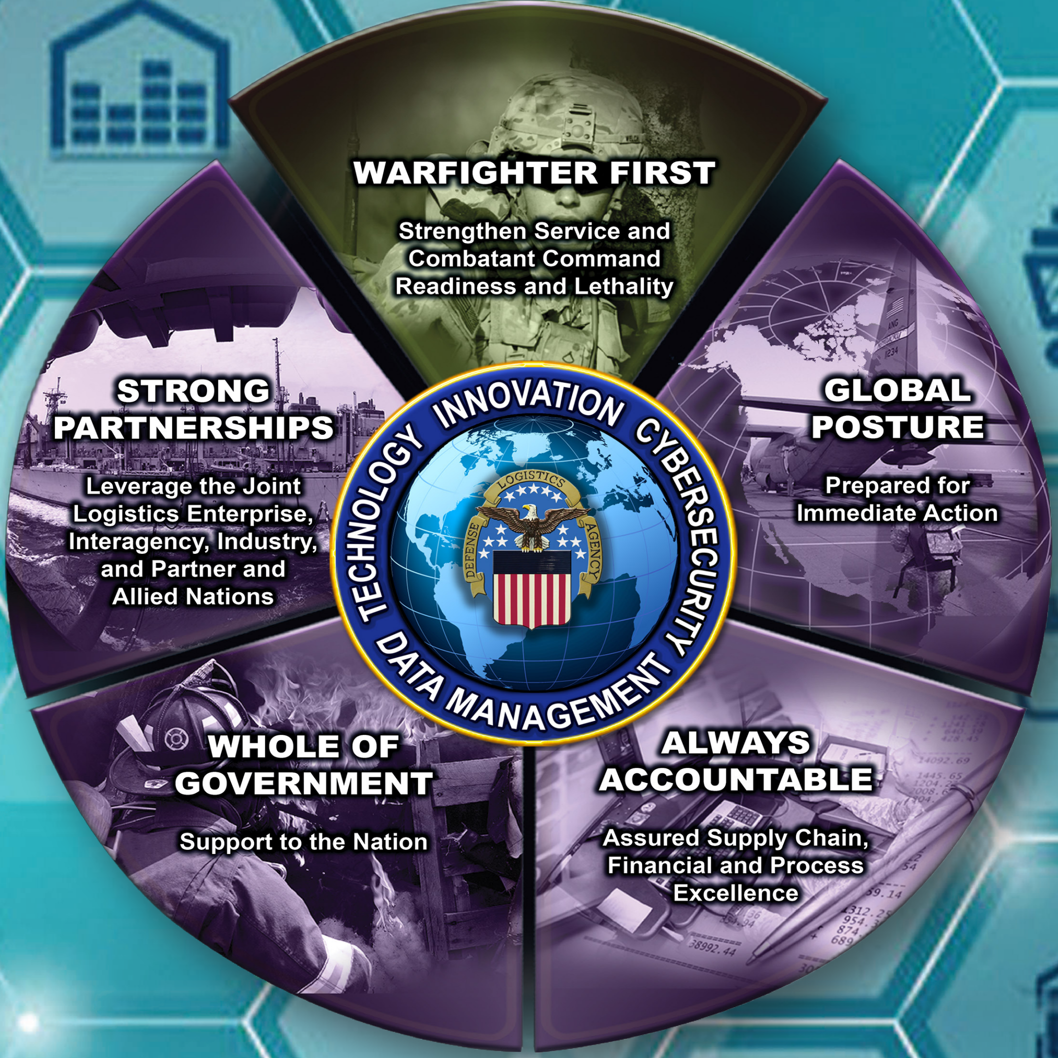
By *institutionalizing Supply Chain Security*, DLA will have the ability to manage supply chain risk at the enterprise-level by fully integrating it into the Mission Assurance portfolio and Enterprise Risk Management framework.

By *maintaining integrity and access to key data*, DLA will develop offensive and defensive mitigating solutions that protect the Agency's data for internal use and strengthens OPSEC by controlling the exportation of DLA's data to external partners.

By *partnering with reputable vendors*, DLA will develop offensive and defensive mitigating solutions that prevent counterfeit parts from entering into DLA's Global Supply Chain and ensure that the vendors DLA partners with produce high-quality materiel for the Warfighter.

By *strengthening the resiliency of systems, processes, infrastructure and people*, DLA will ensure that support to the Warfighter continues even in the midst of disruptive activity by strengthening operational resiliency across the Global Supply Chain.

Warfighter First!



WARFIGHTER FIRST

Strengthen Service and Combatant Command Readiness and Lethality

GLOBAL POSTURE

Prepared for Immediate Action

ALWAYS ACCOUNTABLE

Assured Supply Chain, Financial and Process Excellence

WHOLE OF GOVERNMENT

Support to the Nation

STRONG PARTNERSHIPS

Leverage the Joint Logistics Enterprise, Interagency, Industry, and Partner and Allied Nations

INNOVATION • CYBERSECURITY • DATA MANAGEMENT • TECHNOLOGY

The Nation's Combat Logistics Support Agency

8725 John J. Kingman Road • Fort Belvoir, Virginia • 22060

www.dla.mil • www.facebook.com/dla.mil • www.twitter.com/dlamil • www.youtube.com/user/dodlogisticsagency