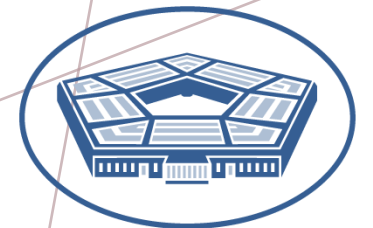




A2A INTEGRATED LOGISTICS INC

PRESENTS

GOLDILOCK FIREBREAK



U.S. Department of Defense

A2A INTEGRATED LOGISTICS INC

- Founded in 2010
- SDVOSB Certified & 8(a) Participant
- Strategic Partnerships & Global Operations
- 40+ years of military experience from leadership
- CEO/Founder – Mr. Anthony “Tony” Bryant



**Integrated
Logistics**
"UNCONDITIONAL SUPPORT"

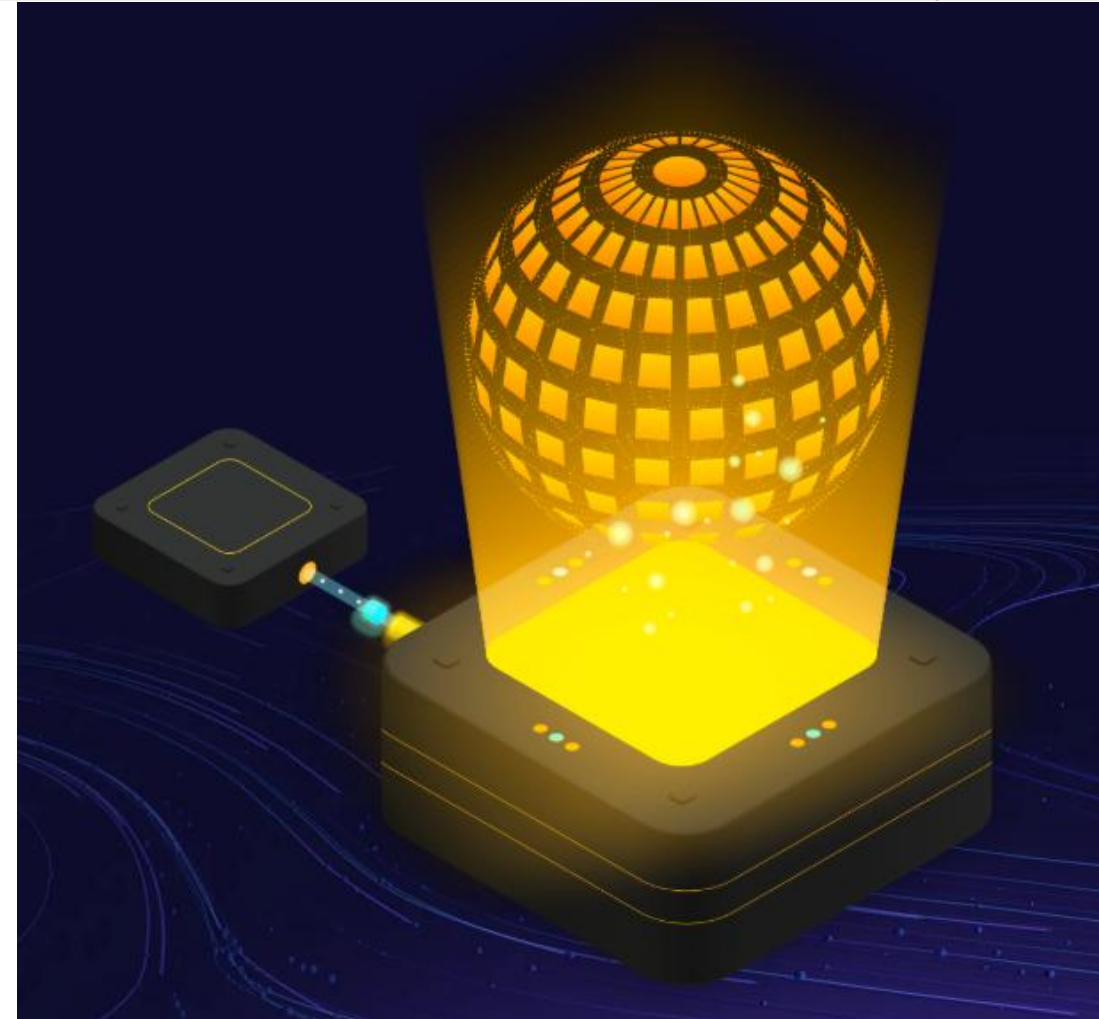
GOLDILOCK FIREBREAK

TRUE PHYSICAL DISCONNECTION



GOLDILOCK FIREBREAK

- HOW GOLDILOCK INNOVATES
- WHY GOLDILOCK WAS CREATED
- WHATS UNIQUE ABOUT GOLDILOCK
- TECHNICAL READNIESS LEVEL



CONTINUED.....

- BENEFITS OF AIR-GAPPING
- IMPORTANCE OF AIR-GAPPING
- STRATEGIC PLACEMENT OF FIREBREAK



GOLDILOCK FIREBREAK

ACTIONABLE USE CASES



CYBER ATTACKS INCREASE

CYBER ATTACKS INCREASE

1.1: 70% increase in cyberattacks on U.S. utilities

1.2: Grid expansion and digitalization are increasing exposure to cyber threats

1.3: Outdated software



#1 - POWER GRID PROTECTION

GRID CHALLENGES

- 1.1: Nation State Threats
- 1.2: Physical and Cyber Convergence
- 1.3: Legacy Systems
- 1.4: Operational Continuety
- 1.5: Access Control



POWER GRID PROTECTION

GOLDILOCK SOLUTION

1.1: Cyber Vault for OT Systems

1.2: Time-Based and Role-Specific Access

1.3: Immutable Configuration Backups

1.4: Network Segmentation and Threat Containment

1.5: Asset Hiding and Attack Surface Reduction



POWER GRID PROTECTION

GOLDILOCK BENEFITS

1.1: Mission Assurance and Zero-Trust Enforcement

1.2: Operational Resilience and Advanced Threat Detection

1.3: Compliance Ready



DEFENSE INDUSTRIAL BASE

KEY FACTS

1.1: 100,000+ companies form the DIB

1.2: 1.6 million jobs across the U.S.
supply chain

1.3: 25,000 to 30,000 small businesses

1.4: Supply chain vulnerabilities



#2 - DEFENSE INDUSTRIAL BASE THREATS

RISING THREATS & NOTABLE INCIDENTS

- 1.1: Exfiltration of DoD blueprints and weapons designs
- 1.2: Spear-phishing and ransomware attacks
- 1.3: Advanced persistent threats (APTs)
- 1.4: Third-party software compromises



#2 - DEFENSE INDUSTRIAL BASE THREATS

GOLDILOCK KEY CAPABILITIES & CONCLUSION

1.1: Layer 1 Physical Isolation

1.2: Micro-Segmentation for Critical
Systems

1.3: Zero Trust Enforcement

1.4: Kill Switch / Drawbridge
Functionality



ALIGNING WITH DISA'S STRATEGIC PLANNING FRAMEWORK



DISA STRATEGIC IMPARATIVES



1. Operate and Secure the DISA Portion of the DOD Information Network

**1.1: PROVIDE RELEVANT, MODERN
ENTERPRISE AND BUSINESS TOOLS**

**1.2: PROVIDE RESILIENT AND REDUNDANT
DEFENSE INFORMATION SYSTEM NETWORK
BACKBONE**

1.3 MANAGE THE AGENCY

DISA STRATEGIC IMPARATIVES



2: Support Strategic Command, Control and Communications

2.1: OPERATIONALIZE THE CLOUD

DISA STRATEGIC IMPARATIVES

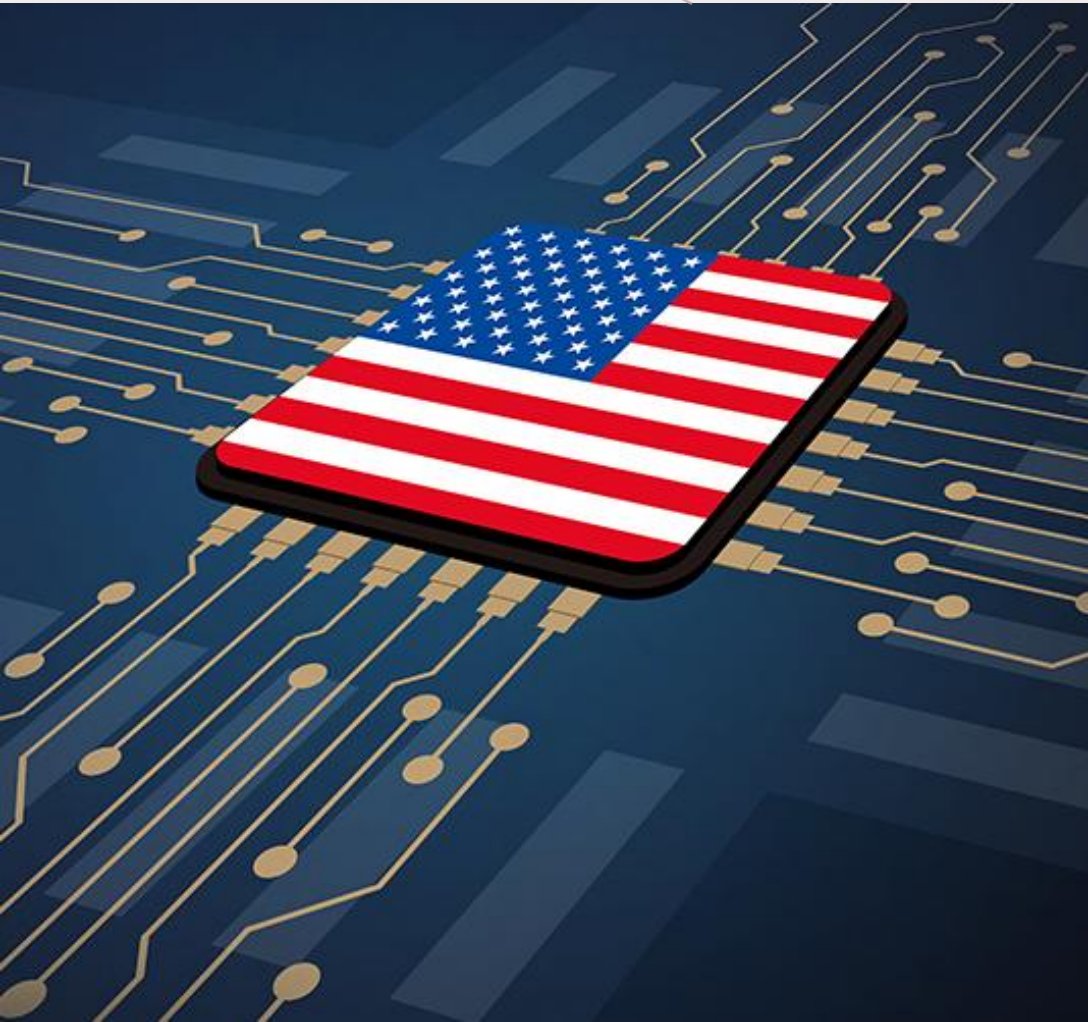


3: OPTIMIZE THE NETWORK

3.1: UNIFY THE NETWORK

3.2: DIVEST TECHNICAL DEBT

DISA STRATEGIC IMPARATIVES



4: Operationalize Data

4.1: Proactively collecting, storing, correlating and interpreting data

TECHNICAL PRESENTATION

The background features several thin, brown lines that intersect to form various geometric shapes, including triangles and polygons, creating a modern, abstract design.

QUESTIONS?

A2A INTEGRATED LOGISTICS CONTACTS

- CEO - Anthony “Tony” Bryant / Phone: (973)527-5299 / Email: tbryant@a2a-logistics.com
- VP Business Development – Gabriel Curtier / Phone: (864)875-0221 / Email: gcurtier@a2a-logistics.com

