Fraud Risk and Supply Chain Risk Management (SCRM): Counterfeit Parts on the Flightline

Deborah Houchins
SAF/GCR
25 August 2025

Agenda

- Introduction
- Fraud Risk Management Approach
- Potential Risks on the Flightline
- Cyber, Data Analytics, and the Compelling Case for Data Strategy
- Supply Chain Risk Management
- Closing

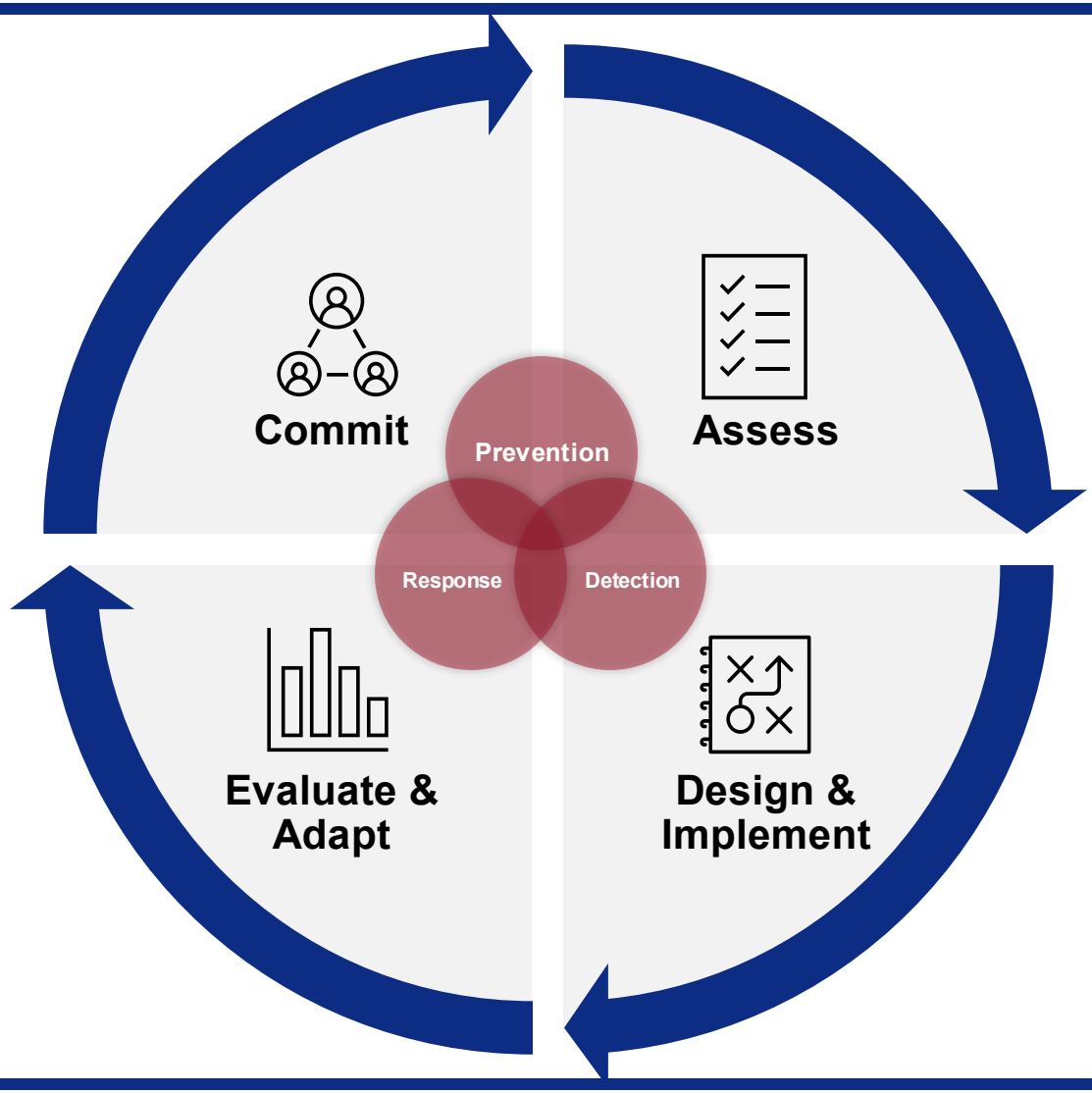
Fraud Risk Management Approach

GAO FRM Framework

GAO's Fraud Risk Framework:

Created to help federal government management combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework called the Fraud Risk Management Framework.

- GAO FRM Framework



Potential Fraud Risks on the Flightline

Flightline Relevant Potential Risk Areas

The DAF's exposure to counterfeit parts extends beyond the physical degradation of mission systems. It directly intersects with cybersecurity vulnerabilities and operational readiness. Our analysis considers both the technical and supply chain dimensions, providing a prioritized view of where counterfeit parts infiltration could most severely undermine readiness, compromise sensitive data, or disrupt mission execution.

High Risk Areas

- Infiltration of mission-critical systems through counterfeit avionics parts
- Cyber backdoors in counterfeit network components
- Loss of sensitive design data during procurement process

Moderate-Risk Areas

- Supplier non-compliance with cybersecurity clauses
- Delays in readiness from quality failures

Low-Risk Area

- Non-electronic replacement parts with minimal cyber-risk exposure

Potential Flightline Recommendations

- **Quick Wins (Items that can be completed within 6 months)**
  - Enhance supplier verification processes and implement enhanced part authentication (blockchain could be utilized for security)
  - Immediate audit of suppliers handling mission-critical components
  - Increased cybersecurity training for procurement and maintenance staff
- **Long Term Strategies (Items that may take multiple years to implement)**
  - Implement AI-driven anomaly detection for supply chain data
  - Create a DAF-wide counterfeit part detection and response framework
  - Enhanced investment area: secure, vetted supplier networks with continuous cyber risk monitoring

Cyber, Data Analytics, and the Compelling Case for Data Strategy

A Paradigm Shift

- **Zero Trust (ZT) – Assume nothing, check everything, and limit access**
  - A key requirement for zero trust is that the enterprise consistently collects, inspects, and analyzes traffic across its entire ecosystem, ensuring maximum real-time visibility into both the data that users can access and the potential for malicious activity.
  - Zero Trust Strategy
  - Zero Trust Execution Roadmap

Zero Trust

- ZT is the term for an "**evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources**." At its core, ZT **assumes no implicit trust is granted** to assets or users based solely on their physical or network location (i.e., local area networks versus the Internet) or asset ownership (enterprise or personally owned). This shift in philosophy is a **significant change in legacy authentication** and security mechanisms. It also represents a **major cultural change** that stakeholders throughout the DoD ZT Ecosystem, including the Defense Industrial Base, will need to embrace and execute beginning with FY2023 through FY2027 and in the future.

Emerging Trends

Generative AI

Synthetic Identities

Fraud as a Service (FAAS)

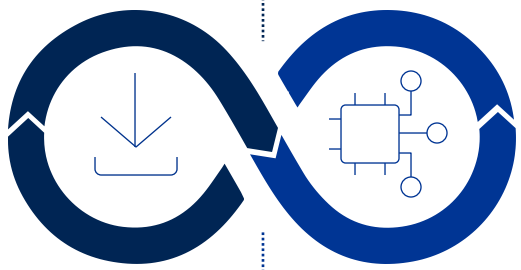
Emerging Trends – Generative AI

What does this mean for fraud?

- It is even easier than ever to create convincing false or misleading documents and data.
- GenAI has drastically increased the speed, sophistication and persistence of traditional fraud, and allows for far more effective social engineering schemes (deepfakes, forgery, phishing, etc.).

Deepfakes:

- Synthetic media created by manipulating real images, videos, or audio. They can convincingly mimic real people's faces, voices, or movements, resulting in altered media that appears authentic. Deepfakes can be done in real time using AI.



AI Enhanced Digital Forgery:

- Counterfeited documentation isn't new to the fraud space, but with Gen AI the barriers are lower than ever. Historically, technical barriers limited the ability to create fake documentation even when the motivation existed. Now we can't rely on traditional visual cues to identify fake financial documents.

Emerging Trends – Generative AI

One document is a genuine transaction and the other was created using ChatGPT

Can you spot the fake?

Emerging Trends – Synthetic Identities

- **What are they?** Synthetic Identities are fake identities that are manufactured using a combination of real personal information and fraudulent or fabricated information. Synthetic ID fraud creates fabricated identities using names, addresses, birthdates, and Social Security Numbers (SSNs) from different people. Synthetic identities can also be created for businesses.
- **Victims often include the young, the elderly, and the homeless (individuals less likely to use or check their credit).**
- **Several factors have contributed to the rise:**
  - The rise in PII (personally identifiable information) available on the dark web and on fraud forums.
  - The change to randomly assigned social security numbers versus using an algorithm. This was not only changed to help prevent fraud, but it also led to an increase in difficulty in identifying synthetic identities.

The Deloitte Center for Financial Services estimated that in the U.S. alone, synthetic identity fraud will generate at least **$23 billion in losses by 2030**.

The Federal Reserve estimates that **40% of synthetic IDs** use post-randomized SSNs, and some brokers even sell currently unassigned SSNs on the dark web as well.

Emerging Trends – Fraud as a Service (FaaS)

■ What fraud methods are FaaS providers using?	
Online Payment Fraud	Payment fraud occurs when a fraudster uses stolen credit card details and personal information to carry out online transactions without the cardholder's consent. A criminal who wants to carry out online payment fraud can do so by purchasing stolen credit card numbers and other details from a FaaS business.
Account Takeover	An account takeover occurs when someone logs into and uses an account that isn't theirs. It can be done to impersonate the account owner, access sensitive personal information, conduct business email compromise (BEC) fraud, and more. Instances of account takeover fraud are increasing, with estimates suggesting that 22% of adults in the U.S. have fallen victim to it, with average losses in the region of $12,000 per case, according to Security.org. Cybercriminals who don't want to hack into accounts and take them over themselves can pay FaaS providers to do it for them.
Account Farming	Account farming is when fraudsters build up and maintain banks of online accounts, such as accounts for webmail services or social media sites. FaaS providers use automated tooling and processes to do this at scale, resulting in a bank of active, trusted accounts that they can sell to clients.

Emerging Trends - FaaS/ Account Takeover

Account Take Over

- Account takeover fraud (ATO) occurs when a cyber attacker gains control of a legitimate account.
- ATO is characterized by unauthorized individuals taking over someone else's online account — such as a bank account, email account, or social media profile — without the account owner's permission.
- This criminal activity is achieved by obtaining the account holder's login credentials through different types of attacks, including phishing, malware attacks, social engineering, or data breaches.

ATO / Identity Theft

- ATO is a type of Identify Theft in which a criminal steals a business's or individual's valid online banking credentials and then uses those credentials to initiate funds transfers out of the account.

How it's performed

- Identity and Data Theft will most likely start with a fraudster trying to gain access to an individual's personal information (e.g. full name, address, date of birth, social security number, etc.) in order to steal the individual's identity and proceed with financial activities (e.g. banking, mortgage, investments, etc.) for personal gain.

DISA Data Strategy

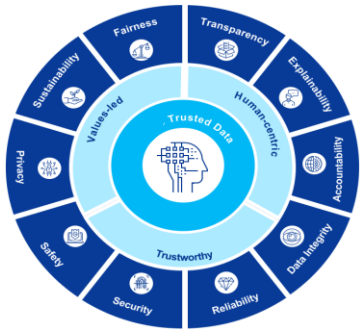
Objective: To establish a solid base for managing, analyzing, and using data to boost mission readiness, operational efficiency, and provide timely, accurate intelligence to the Warfighter by:

- **Strengthening Data Architecture and Governance**
  - Enhances mission readiness
  - Increases operational efficiency
  - Safeguards the integrity of our information assets
- **Integrating Advanced Analytics**
  - Transforms raw data into actionable insights that drive growth
  - Optimizes efficiency and creates a competitive advantage
- **Cultivating a Data-Centric Culture**
  - Empowers our workforce with the skills, tools, and training necessary to harness the full potential of data, fostering collaboration, continuous learning, and a commitment to using our data for decision-making

DISA Data Strategy FY25-27

Data Strategy Outcomes

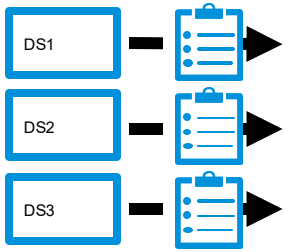
Define Data Strategy → **Discovery / Define Use Cases** → **Establish Governance and Standards** → **Architect Data Environment / Data Ingestion** → **Develop and Deploy Data Products** → **Serve and Deliver Insights** → **Consume and Improve**



Define Data strategy and establish clear milestones and objectives

Data Users, Customers, etc.

Stakeholder Interviews



Identify and prioritize business use cases with greatest potential for impact and highest feasibility

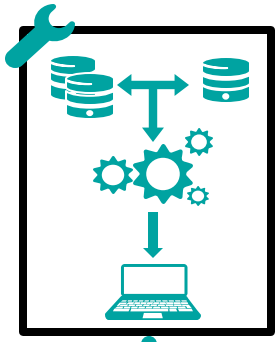
1. Use of Analytics and SCRM Techniques for fraud risks
2. Cybersecurity to protect data to reduce capability to counterfeit (protecting that IP)
3. Risk of cyber counterfeiting inside cyber enabled platforms like satellites and next gen aircraft

Data Lifecycle Management - Master Data Management, Data Catalog, Data Security & Privacy

Establish proper governance and policies to ensure data ownership, quality, and compliance. Define data-related roles and responsibilities.

Data Sources, Target Systems, Data Ingestion & Metadata Management

Architect and enable requisite data environment architecture to fulfil technical data requirements



Develop data models, transformations, data products, and foundation to support use cases for advance analytics including Generative AI.

Visualizations & Reports, Advanced Analytics (AI/ML), Gen AI

Enable organizations to derive actionable insights from their data through advanced analytics includes data visualization, predictive analytics, machine learning and generative AI to uncover patterns, trends, and opportunities for business growth.

Data Driven Culture

Data Outcomes:

- Early ID of Fraudulent Activities
- Advanced Risk Profiling and Segmentation
- Enhanced Operational Efficiency in Fraud Investigation
- Real-Time Fraud Detection Capabilities
- Predictive Analytics for SCRM Capabilities

Data Analytics Requirement

- **"DoD Fraud Risk Management Strategy and Guidance" (June 2025) requires DoD components to:**
  - **Develop an action plan to implement data analytics by Q3 FY2026**
  - **Fully implement data analytics activities by YE FY2027**

- **See Para. 2.5:**

> ***2.5 Component Data Analytics Requirements***
>
> At a minimum, Components will be required to develop an action plan with milestones to implement Government Purchase Card (GPC), Government Travel Card (GTC), Improper Payment and Procurement Fraud data analytics activities. The action plan must be completed no later than the third quarter of FY 2026 and will be submitted to the RMIC SharePoint site via the Statement of Assurance Execution Handbook instructions. All required data analytics activities will be fully implemented no later than the end of FY 2027.

Supply Chain Risk Management

Supply Chain Risk Management (SCRM)

- SCRM is the systematic process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions throughout the supply chain and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as threats are identified or disruptions occur.
- The following steps represent best practices in executing SCRM:
  - Step 1: Integrate SCRM into a Program Lifecycle
  - Step2: Assess Supply Chain Vulnerability
  - Step 3: Assess Threats – Obtain Service Intelligence Products or DIA SCRM TAC Assessments
  - Step 4: Capture Risks in Risk Register
  - Step 5: Determine Risk Response
  - Step 6: Create Risk Mitigation Plan
  - Step 7: Capture Response Actions and Results in Risk Register
  - Step 8: Continually Monitor Supply Chain Risk

SCRM Guidance

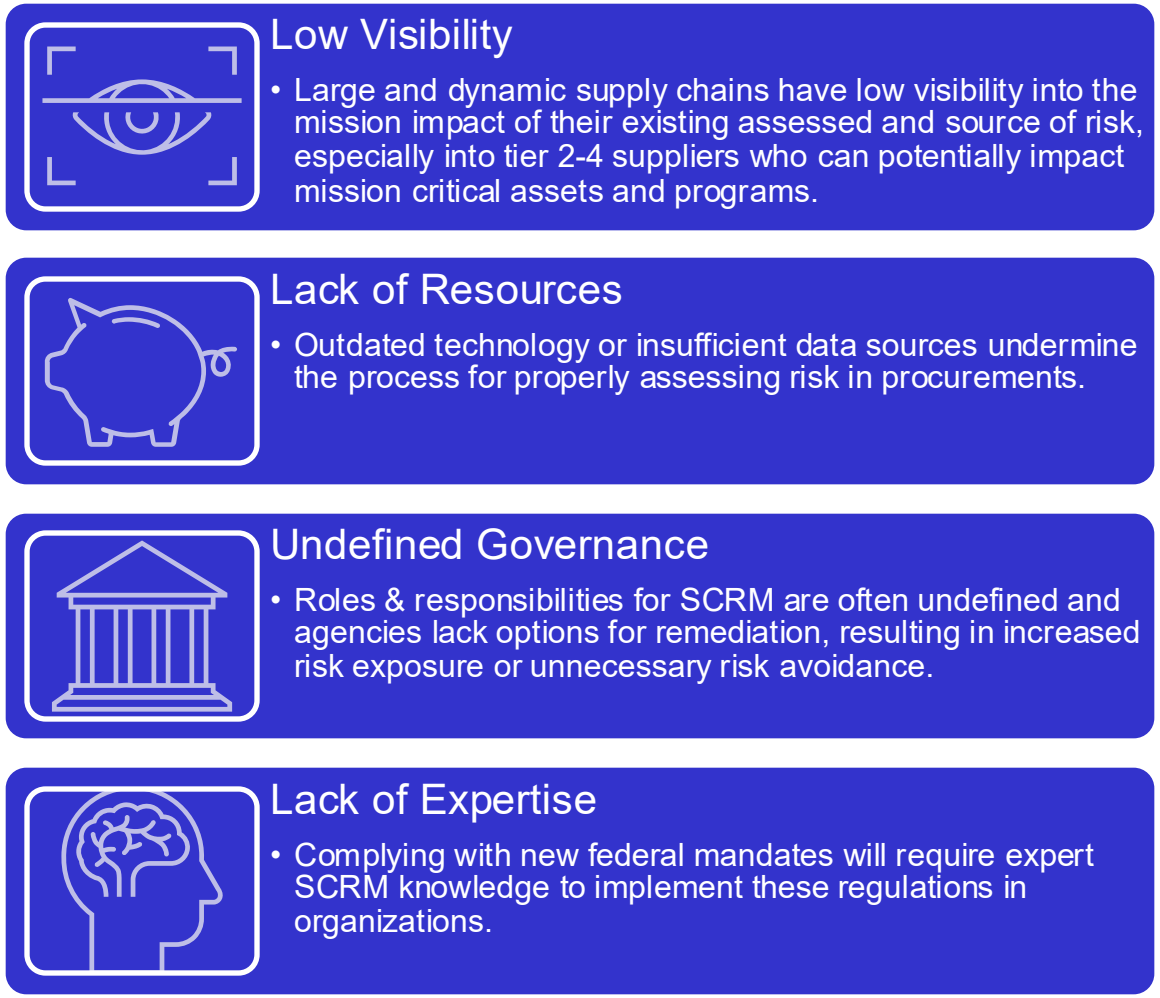
- **OMB M-22-18**, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (September 2022),* directs implementation of SCRM-specific elements of EO-14028 and NIST guidance.

  - **Executive Order (EO) 14028 Section 4e**, *Improving the Nation's Cybersecurity (May 12, 2021)*, focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the NIST to issue guidance "identifying practices that enhance the security of the software supply chain."

  - ***NIST Guidance on Section 4e & Secure Dev. Framework (July 2021 & February 2022),*** provides a guide to follow for creating a risk-based approach to secure software development and steps to take to securely design.

Challenges Facing Supply Chains

- **Federal mandates and industry best practices dictate the federal agencies implement comprehensive SCRM programs to ensure compliance, security, and resilience in their supply chains.**
- **The graphic to the right illustrates some of the challenges faced in managing supply chain risk:**



Federal Supply Chains Do Not Meet Tomorrow's Challenges

Supply Chain Issues

- Limited Supply Chain Visibility
- Challenging Inventory Management
- Inefficient Operations
- Highly Manual Operations - Excess Labor
- Poor demand signals
- Supply Chain disruption
- Unreliable supply

Emerging Challenges

- Aging fleet
- Pressure to do more with less and with accountability (FIAR)
- Efforts to automate, digitize, and create efficiencies
- Supporting readiness and logistics in a contested environment

""The line between disorder and order lies in logistics" attributed to Sun Tzu

Solution: Harnessing Data Analytics

Use Case: Use of Analytics and SCRM Techniques to Find Fraud Risks

1. Analytics for Early Fraud Detection and Prevention
2. Risk Assessment and Prioritization
3. Continual Monitoring

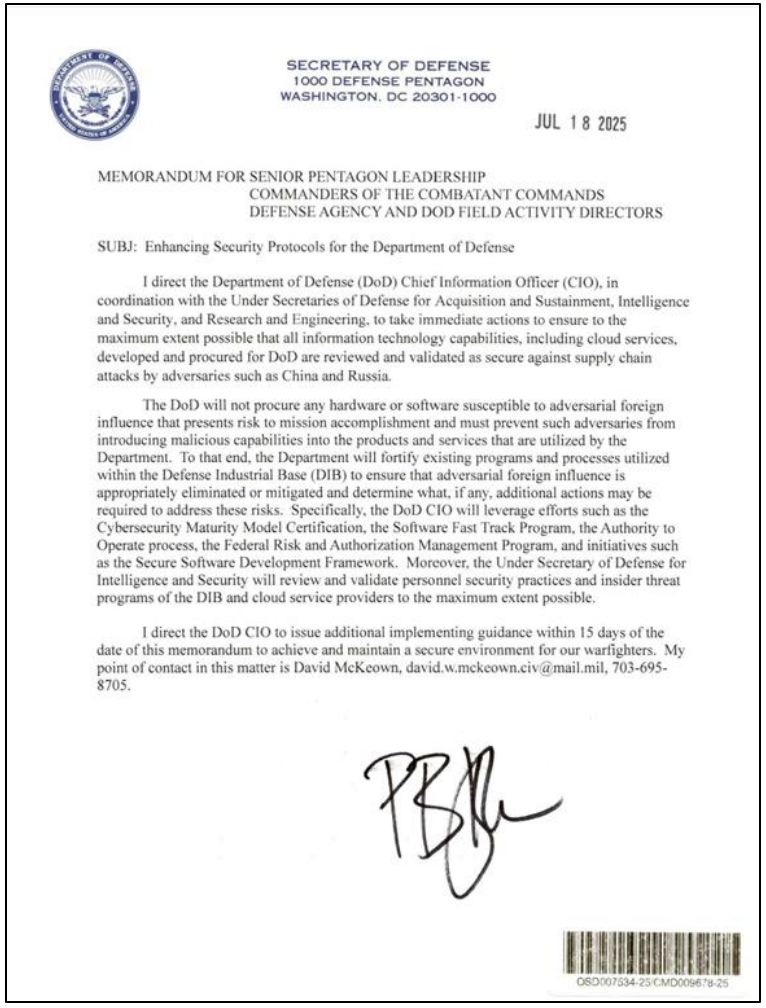
Use Case: Cybersecurity to Protect Data and Reduce Capability to Counterfeit (Protecting IP):

1. Securing Information Systems
2. Policy Implementation
3. Collaboration and Information Sharing

Use Case: Risk of Cyber Counterfeiting Inside Cyber Enabled Platforms Like Satellites and Next Gen Aircraft

1. Vulnerabilities in High-tech Platforms
2. Rigorous Supply Chain Evaluation
3. Integration of Advanced Cybersecurity Measures

Solution: Enhancing Security Protocols for the DoD



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUL 18 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJ: Enhancing Security Protocols for the Department of Defense

I direct the Department of Defense (DoD) Chief Information Officer (CIO), in coordination with the Under Secretaries of Defense for Acquisition and Sustainment, Intelligence and Security, and Research and Engineering, to take immediate actions to ensure to the maximum extent possible that all information technology capabilities, including cloud services, developed and procured for DoD are reviewed and validated as secure against supply chain attacks by adversaries such as China and Russia.

The DoD will not procure any hardware or software susceptible to adversarial foreign influence that presents risk to mission accomplishment and must prevent such adversaries from introducing malicious capabilities into the products and services that are utilized by the Department. To that end, the Department will fortify existing programs and processes utilized within the Defense Industrial Base (DIB) to ensure that adversarial foreign influence is appropriately eliminated or mitigated and determine what, if any, additional actions may be required to address these risks. Specifically, the DoD CIO will leverage efforts such as the Cybersecurity Maturity Model Certification, the Software Fast Track Program, the Authority to Operate process, the Federal Risk and Authorization Management Program, and initiatives such as the Secure Software Development Framework. Moreover, the Under Secretary of Defense for Intelligence and Security will review and validate personnel security practices and insider threat programs of the DIB and cloud service providers to the maximum extent possible.

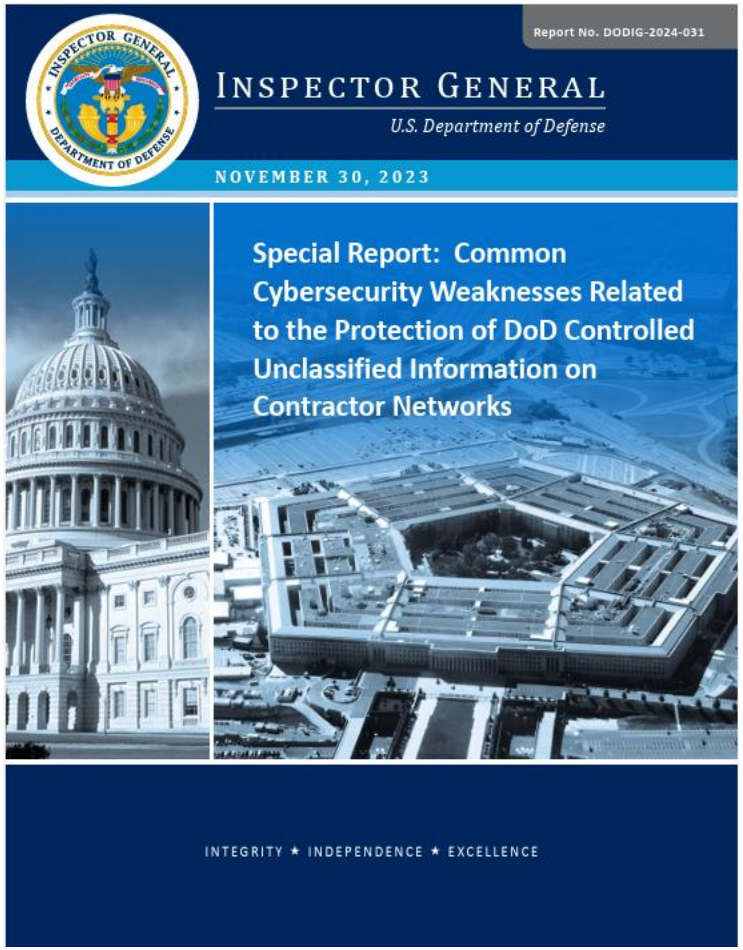
I direct the DoD CIO to issue additional implementing guidance within 15 days of the date of this memorandum to achieve and maintain a secure environment for our warfighters. My point of contact in this matter is David McKeown, david.w.mckeown.civ@mail.mil, 703-695-8705.

OSD007534-25/CMD009678-25

Directs the DoD to take immediate actions to ensure to the maximum extent possible that all information technology capabilities, including cloud services, developed and procured for DoD are reviewed and validated as secure against supply chain attacks by adversaries.

To that end, the Department will fortify existing programs and processes utilized within the Defense Industrial Base (DIB) to ensure that adversarial foreign influence is appropriately eliminated or mitigated and determine what, if any, additional actions may be required to address these risks.

Solution: Addressing Third-Party Challenges



Requirement:

- NIST SP 800-171 requires the protection of controlled unclassified information in nonfederal systems and organizations

Common Findings Among DoD Contractors:

- Multifactor Authentication/ Strong Passwords
- System Activity and User Activity Reports
- Disabling Inactive User Accounts
- Physical Security
- Network & System Vulnerabilities
- Scanning for Viruses & Malicious Code

Solution: Vendor Risk Management

Foundational:

"Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the intent of the USG to allow foreign investment consistent with the national security interests of the United States."

– 32 CFR 117.11

Why Due Diligence is a good idea?

- **Ensures the reliability, compliance, and quality of services provided by third-party vendors**
  - **Mitigates Risk**
  - **Quality Assurance**
  - **Reputation Management**
  - **Cost Effectiveness**

How do we get there?

- **Conduct due diligence on high-risk vendors and grantees, reviewing financial stability, ownership, and past performance issues**
- **Discover hidden relationships, cyber threats, insider threats, and risk from foreign ownership that may enable fraud**
- **Continuously monitor vendor transactions and performance to detect billing fraud, product substitution, and other schemes**
- **Identify vendor relationships posing fraud or reputational risk**

Any Questions?

Contact Information:

Deborah Houchins

Associate General Counsel

E: deborah.houchins.1@us.af.mil

P: (703) 697-1905

"Collaboration between cybersecurity and fraud prevention is not just a harmonious alliance — it's an essential strategy for safeguarding the digital realm against the evolving tactics of modern criminals."

- Kennedy Meda, "Unifying forces: The synergy of cybersecurity and fraud prevention teams" (4 Jan 2024)