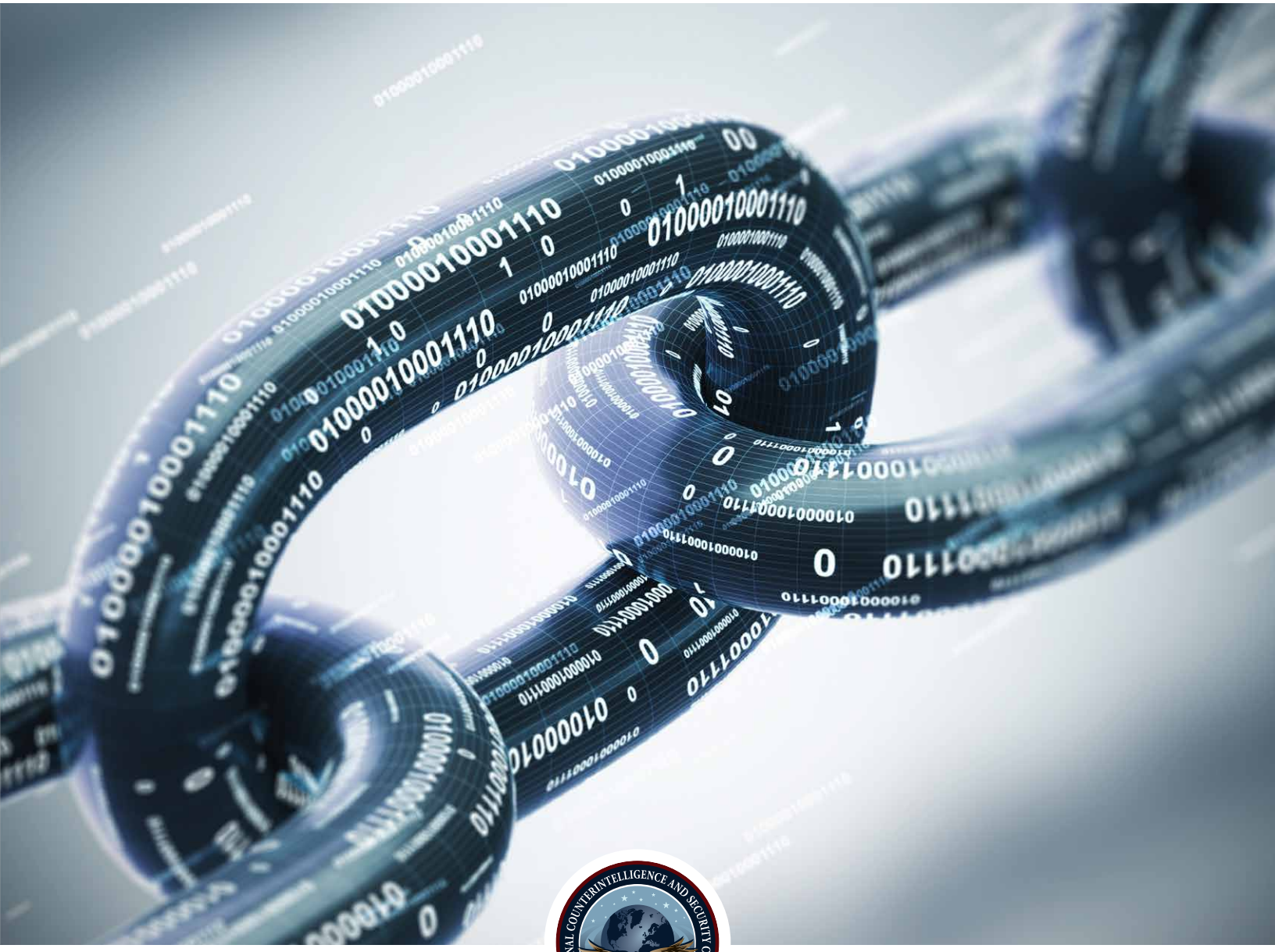
Supply Chain Risk Management:

Reducing Threats to Key U.S. Supply Chains



NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

One of the five pillars of the National Counterintelligence Strategy of the United States 2020-2022:

Reduce Threats to Key U.S. Supply Chains

The National Counterintelligence Strategy of the United States 2020-2022 strategic objective for supply chain security is to: "Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base, and the private sector.

The exploitation of key supply chains by foreign adversaries—especially when executed in concert with cyber intrusions and insider threat activities—represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure.

Foreign adversaries are attempting to access our nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by inserting malware into important information technology networks and communications systems.

The increasing reliance on foreign-owned or controlled hardware, software, or services as well as the proliferation of networking technologies, including those associated with the Internet of Things, creates vulnerabilities in our nation's supply chains. By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry, or even subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis. We must elevate the role of supply chain security in the acquisition process.

TO MEET THIS OBJECTIVE, THE U.S. GOVERNMENT WILL:

Enhance capabilities to detect and respond to supply chain threats. We will develop access to new sources of information and increase the analytic capacity to understand and assess foreign intent and capability to exploit U.S. supply chains. We will also implement new processes to identify suspect or high risk vendors, products, software and services that pose a risk to our economic and national security.

Advance supply chain integrity and security across the federal government. We will integrate Supply Chain Risk Management capabilities and processes consistent with industry best practices into the operations of the federal government to safeguard the technology and services that are procured and deployed. We will create a supply chain risk assessment shared repository, address deficiencies in the federal acquisition process, and seek more streamlined authorities to exclude high risk vendors.

Expand outreach on supply chain threats, risk management, and best practices. Through expanded outreach and sustained engagement, we will establish and deepen partnerships with state, local, tribal, and territorial governments, and the private sector, and share supply chain threat information and mitigation measures with our partners, especially in U.S. critical infrastructure sectors.

Key Supply Chains: Defending and Mitigating Risks

WHAT IS A KEY SUPPLY CHAIN?

A supply chain is a network of people, processes, technology, information, and resources that delivers a product or service. Key supply chains are essential to protecting critical infrastructure; countering economic exploitation; and defending against cyber and technical operations. One key supply chain is the information and communications technology (ICT) supply chain because it supplies the hardware, software, firmware, networks, systems, and services that underpin the U.S. Government and the private sector.

WHAT ARE SUPPLY CHAIN RISKS?

A supply chain risk is a function of threat, vulnerability, and consequence. A supply chain threat is specific and credible information that a component, system, or service might be targeted by adversaries. A vulnerability is a weakness which is either inherent to the component, system or service, or has been introduced by an outside agent.

A supply chain risk is when the capability and intention of an adversary aligns with the opportunity to exploit a vulnerability. The consequence of this would allow the adversary to extract Intellectual Property (IP), sensitive government data, and personally-identifiable information. Further, such an action may allow an adversary to surveil, deny, disrupt, or otherwise degrade a component, system, or service. These actions may compromise the integrity, trustworthiness, and authenticity of critical ICT services and products.

Risks to the supply chain are functions of threat, vulnerability and consequence.

WHAT IS SUPPLY CHAIN RISK MANAGEMENT?

Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the risks to the integrity, trustworthiness, and authenticity of products and services within the supply chain.

Three Focus Areas to Reduce Threats to Key U.S. Supply Chains:

1. Enhance Capabilities to Detect and Respond to Supply Chain Threats

2. Advance Supply Chain Integrity and Security across the Federal Government

3. Expand Outreach on Supply Chain Threats, Risk Management, and Best Practices

1. ENHANCE CAPABILITIES TO DETECT AND RESPOND TO SUPPLY CHAIN THREATS

The supply chain is one avenue whereby adversaries might threaten U.S. national and economic security interests. To minimize the threats to key supply chains, existing threat detection, response, and mitigation tools should be leveraged across all aspects of the lifecycle. These tools and capabilities should be optimized for specific supply chains. In addition, new tools and technologies should be developed to:

- Provide automatic updates to threat information and risk mitigations
- Enable rapid detection and automatic response to threats
- Incorporate Artificial Intelligence/Machine Learning to increase agility

Tools and Technologies to Protect each Stage of the Supply Chain Lifecycle

CONTENT & DESIGN

Zero Trust Architecture:
- Firewalls
- Data Encryption
- Continuous Monitoring

Validation & Verification

MANUFACTURE & INTEGRATION

Unique Product ID
- Barcodes
- Radio Frequency ID (RFID)
- Digital Markers

Zero Trust Architecture

DEPLOYMENT

Tamper-Evident Tapes & Seals

GPS, Bluetooth Tracking

MAINTENANCE

Access Controls

Zero Trust Architecture

RETIREMENT

Asset Management

Data Destruction Tools

2. ADVANCE SUPPLY CHAIN INTEGRITY AND SECURITY ACROSS THE FEDERAL GOVERNMENT

To advance supply chain integrity across the federal government, supply chain security must be elevated to a top priority and be present throughout the acquisition process. A robust SCRM program illuminates potential security risks and provides countermeasures to fortify the supply chain. Implementing SCRM programs across the federal government enables an integrated risk-reduction approach to protect supply chains critical to the U.S Government and private industry. Successful SCRM programs need enterprise-wide commitment involving multiple disciplines, comprehensive information sharing, and adherence to best practices.

3. EXPAND OUTREACH ON SUPPLY CHAIN THREATS, RISK MANAGEMENT, AND BEST PRACTICES

Obtain Executive Level Commitment for a Supply Chain Risk Management (SCRM) Program

Build an Integrated Enterprise Team. A successful SCRM program requires commitment from senior stakeholders from across the enterprise including Security, Information Assurance, Insider Threat, Legal, and Acquisition.

Communicate across the Organization. Horizontal and vertical communication is essential to ensure senior stakeholders' investment in the success of a SCRM program. This includes information sharing to inform risk decisions and implement mitigations.

Establish Training and Awareness Programs. Organization-wide awareness and training further embeds the SCRM practices with senior stakeholders and empowers employees to manage, mitigate, and respond to supply chain risks.

Identify Critical Systems, Networks, and Information

Exercise Asset Management. Real-time knowledge of the location and operational status of all assets is essential to understanding what systems, networks, and information are critical to the enterprise.

Prioritize Critical Systems, Networks, and Information. Identifying critical systems, networks, and information enables stakeholders to prioritize resources for protecting these systems and mitigating supply chain risks.

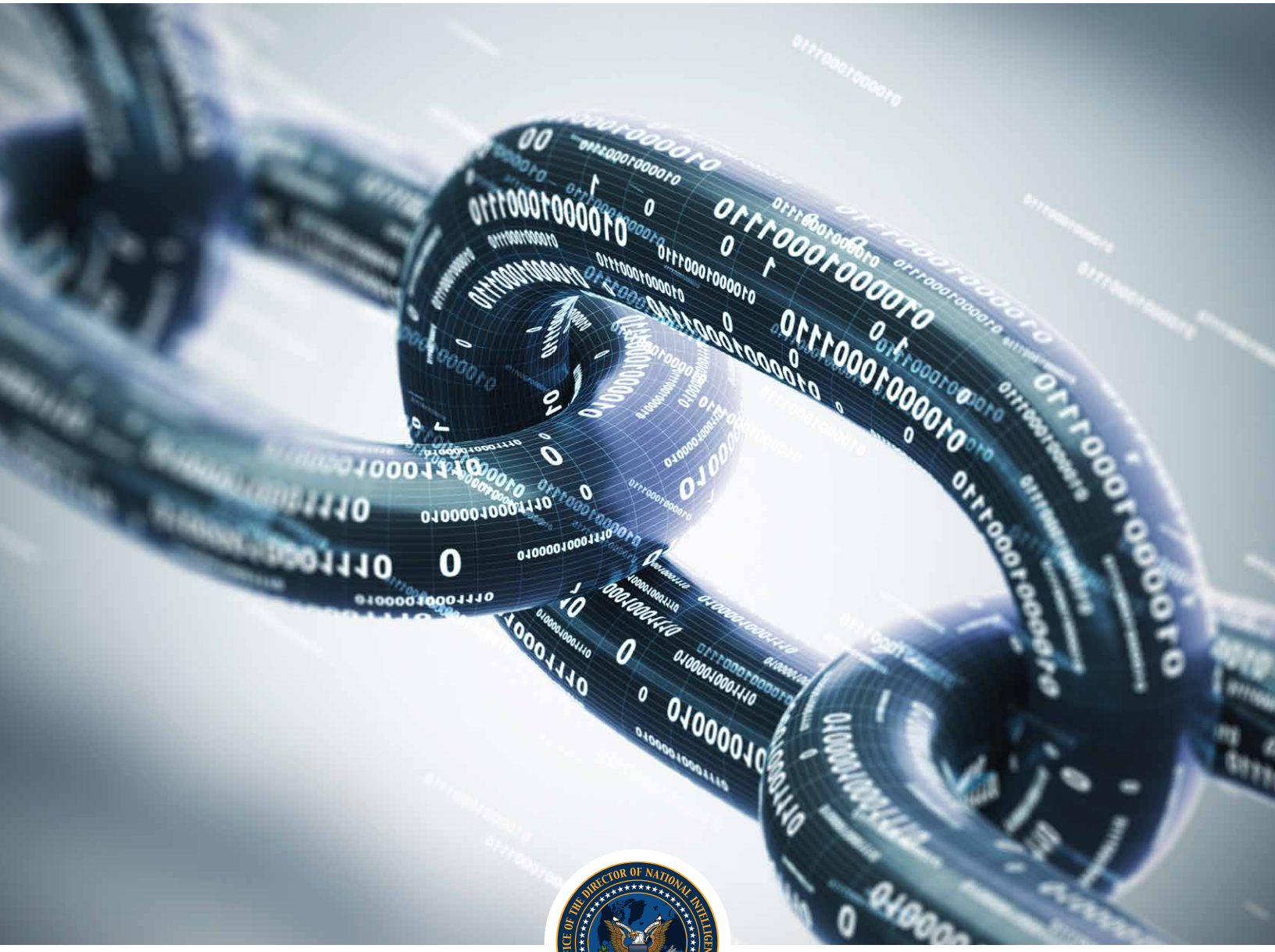
Employ Mitigation Tools. Continuous monitoring of system data and network performance enables rapid implementation of appropriate countermeasures to minimize the impact of an attempted disruption or attack.

Manage Third Party Risk

Conduct Due Diligence. Assess first-tier suppliers regularly to increase visibility into third-party suppliers and service providers. Leverage this data to properly vet vendors who are providing key components to critical systems and networks.

Incorporate SCRM Requirements into Contracts. Use SCRM-related security requirements as a primary metric – just like cost, schedule, and performance - for measuring a suppliers' compliance with the contract. These security requirements include personnel security and system and services acquisition, and are fully described in NIST SP 800-161.

Monitor Compliance. Monitor suppliers' compliance to SCRM-related security requirements throughout the supply chain lifecycle, even when terminating supplier relationships.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE