DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUN 9 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: DoD Commercial-Off-the-Shelf (COTS) Information and Communications Technology Supply Chain Risk Management

The DoD must ensure information and communication technologies (ICT) deployed in every warfighting domain are capable of securely and reliably operating within contested environments. As the Department's ICT risk manager, the Office of the Chief Information Officer (OCIO) is leading this effort. This intensified effort is driven by the need to adapt our cybersecurity and supply chain risk management (SCRM) practices to the rapid pace of software development and the increasing complexity of supply chain risk. We need to accelerate our ability to adopt secure software and technology solutions across all warfighting domains. Current authorization processes often hinder the rapid deployment of critical capabilities, and we lack sufficient visibility into the security and integrity of our increasingly complex technology supply chains.

On March 6, the Secretary of Defense directed all DoD Components to adopt the Software Acquisition Pathway (SWP) as the preferred pathway for all software development components of business and weapon system programs in the Department. This directive recognizes that *software is at the core of every weapon and supporting system we field to remain the strongest, most lethal fighting force in the world*. To that end, on April 24, I initiated a 90-day Software Fast-Track (SWFT) initiative to: (1) define clear, specific cybersecurity and SCRM requirements; (2) establish rigorous software security verification processes; (3) develop secure information sharing mechanisms; and (4) leverage standardized risk determinations to expedite cybersecurity authorizations for rapid software adoption. This initiative directly addresses the need to accelerate secure software adoption within the Department.

Consistent with DoDI 5000.87, "Operation of the Software Acquisition Pathway" the DoD CIO maintains a current knowledge resource listing DoD and DoD Component Enterprise Capabilities available to programs employing the SWP; including the "Requirements for the Acquisition of Digital Capabilities Guidebook". Today, I'm directing an update of this Guidebook concurrent with the SWFT development timeline. This update will build on the 12 risk categories developed by the Office of the Assistant Secretary of Defense for Sustainment (OASD(S)) in Attachment A, to develop a comprehensive framework for managing ICT supply chain risk, including specific considerations to address the unique challenges of the software supply chain.

In addition, the DoD CIO maintains comprehensive ICT-SCRM guidance on https://cyber.mil/ict-scrm. Attachment B outlines key ICT-SCRM requirements DoD components will consider where applicable. While vendor self-attestations are a component of government-wide efforts, DoD is actively exploring and implementing more robust methods for verifying software security. This includes, but is not limited to, independent assessments and more stringent controls for vendors to demonstrate secure software pipeline practices that build on Government and industry standards and best practices.

Katherine E. Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Attachment:
As stated

Risk Categories	**Proposed definition**
1. Regulatory and Compliance	Changes in statutes, laws, policies, regulations, and/or agreements that materially impact a business or market sector and that can increase business operating costs, reduce the attractiveness of investment, or change the competitive landscape. Extends to the inability of a supplier to comply with a wide-arching sets of domestic or foreign statutes, laws, policies, regulations, and/or agreements established to avoid impacts to national security. This can include market practices, contract compliance, fraud, unethical practices, and other actions that are called into moral, ethical, or legal question.
2. Manufacturing & Supply	Either a single supplier or sector/market cannot meet market demand. This can be due to reduced throughput or production delays caused by capacity constraints, obsolescence, industrial limitations, market conditions and the supplier's practices across those markets, disrupted material delivery, and other conditions. Additional concerns include availability of supply, capacity to surge, sole-source, and concentration within or over-reliance on a single source.
3. Foreign Ownership, Control, or Influence (FOCI)	A foreign interest has the power – whether through direct or indirect control, whether or not exercised – to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to information or may adversely affect the performance of contracts and/or programs which support national security.
4. Political	The weakness of political powers and their legitimacy and control; inadequacy of their control schemes, policies and planning, or broad political conditions. May occur due to internal or geopolitical instability, interstate conflict, civil unrest, governmental collapse, political disputes (territorial, trade, etc.), corruption, terrorism, or other factors that can lead to disrupted supply chain operations, increased business operating costs, reduced attractiveness of investment, or altered competitive landscapes.
5. Technology & Cybersecurity	Involves the management of cybersecurity requirements for information and communications technology (ICT) systems, software, and networks, which are driven by threats such as cyber-terrorism, malware, data theft, and the advanced persistent threat (APT). Includes vulnerabilities and exposures of ICT system components produced by a specific supplier. Common risks include weaknesses in computation logic (code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, non-repudiation, or availability.
6. Financial	A supplier cannot generate revenue or income resulting in the inability to meet financial obligations. Financial distress can lead to the inability to meet contractual obligations, hostile takeovers, or bankruptcy.
7. Economic	Factors that influence an economy are out of balance, leading to unpredictable fluctuations in growth, inflation, employment, and financial health. This instability can be episodic, meaning discrete events such as job loss, or it can be chronic, meaning sustained events such as variations to employee compensation. Either way, economic instability can lead to reduced investment and weakened consumer confidence. Multiple factors may cause instability and may include recession, sanctions, demand shocks, price volatility, inflation, and unemployment.

8. Product Quality & Design	Inherent design and quality problems (e.g., raw materials, ingredients, production, logistics, packaging) which result in the item failing to meet performance specifications and quality standards set by industry or DoD. Includes items illegally created and sold under false pretenses. The items lack industry standard tests during the production phase (e.g., pressure testing) or are counterfeit and non-MILSPEC items that could pose significant risk to the function and safety of the system, increased maintenance costs due to depreciation in quality, and added stresses due to an item's inability to function at true capacity.
9. Human Capital	Encompasses the human skills, knowledge, and actions that may impact a market's ability to produce goods and/or services to meet demand. This includes industrial disputes, labor availability and unrest, attrition of required skills, and consumer behavior that disrupts a given market or industry.
10. Environmental	Natural and manmade disasters that may disrupt supply chains. Natural disasters and other extreme weather conditions comprise the bulk of external environmental risk. Manmade disasters can arise from improper health and safety precautions, fires, spills, chemical leaks, and other environmental hazards.
11. Transportation & Distribution	A dynamic disruption within the transportation and logistics of moving a product from one point to another. The transportation industry is among the most risk-prone of all industries due to accidents, losses of cargo, driver shortages, and deteriorating infrastructure. These risks can cause shipment delays, supply chain disruptions, increased costs, and damaged reputations. In addition, the inability to predict and plan for disruptions in the logistics plan presents risk in meeting delivery requirements and maintaining operations.
12. Infrastructure	Consists of the availability and functioning of fundamental facilities and systems necessary to support an industry and its supply chains within a country, such as buildings, transportation networks, utilities, and equipment. Also includes how well those facilities and systems are protected from physical and cyber threats.

Attachment B

This attachment provides ICT-SCRM requirements for DoD components deploying COTS products. DoD components will include the following where applicable:

1. Ensure vendors adhere to NDAA FY19 Section 889 - Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment from Huawei, ZTE, Hytera, Hikvision, Dahua by including FAR clause 52.204-24.
2. In accordance with 15 CFR 7.109(d)(5), ensure products by Kaspersky Labs, and any of its successors and assignees, are excluded by including FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities.
3. For National security systems, verify in SPRS (https://www.sprs.csd.disa.mil/) that none of the proposed products appear on the NSS Restrict list in accordance with 10 U.S.C. 3252 (252.239-7017 Notice of Supply Chain Risk)
4. If a COTS product is identified by National Information Assurance Partnership (NIAP) as approved by a Common Criteria Testing Laboratories (CCTLs) ensure protection profile is implemented and mitigate or resolve identified vulnerabilities. The P-ISSM must also review the technology being accepted or connected as part of the cybersecurity accreditation process to ensure configuration compliance. NIAP validated products can be found here: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm
5. Prioritize software integrity in accordance with OMB Memorandum 22-18. Software integrity is key to protecting Federal systems from nation state and criminal actors seeking to disrupt our nation's critical functions. One way to achieve this is by Federal agencies adopting software from software producers who can attest to complying with the Government-specified secure software development practices, as described in NIST Guidance. The DoD will advocate for voluntary, independent assessments to validate adherence to secure development practices.
6. Validate the minimum NIST SP 800-53r5 controls are implemented in accordance with DoDI 8510.01 and the Assess and Approve baseline in the RMF Knowledge Service (https://rmfks.osd.mil/rmf/RMFImplementation/AssessOnly/Pages/AssessandApprove.aspx).
    a. (SR-2) Supply Chain Risk Management Plan: For any mature implementation of ICT-SCRM, there must be a documented plan to lead an organization's efforts
    b. (SR-3) Supply Chain Controls and Processes: The existence of NIST SP 800-161r1 demonstrates the need for controls and processes to implement ICT-SCRM
    a. (SR-4) Provenance: The ability to manage supply chain risk is fundamentally tied to an ability to know the suppliers of all components and services used for mission execution. The vendor must document, monitor, and maintain valid provenance of the system components and ensure system components are genuine.
    b. (SR-6) Supplier Assessments and Reviews: The ability to determine cybersecurity risk from the supply chain must come from assessments and reviews of suppliers that support the mission
    c. (SR-9) Tamper Resistance and Detection: Implement a tamper protection program for the system, system component, or system service.
7. Obtain the following artifacts as part of the security authorization process:
    a. Hardware and software inventory list
    b. Hardware and device certifications and approvals
    c. Incident response plan
    d. Software Certification test results or attestations/memorandums
    e. Supply Chain Risk Management Policy
    f. List of all implemented STIGs
8. Ensure vendor adheres to the DoD issued Security Requirements Guides (SRG) and any accompanying Security Technical Implementation Guides (STIG).