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

SUBJECT: Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Networks

The DoD works continuously to protect its systems and networks from supply chain risk. All DoD Components are responsible for reviewing and assessing supply chain risk factors, and identifying ways to mitigate those risks during acquisition, sustainment, or integration of capabilities that comprise our trusted systems and networks.

When warranted, DoD leverages the authorities provided in title 10, U.S. Code, section 2339a, to protect its systems and networks from supply chain risk. The DoD published procedures for using those authorities on March 13, 2018.

The attached document modifies these procedures as needed to reflect current statutory references and streamline correspondence requirements. These changes will be integrated into an update of DoD Instruction 5200.44 in the next 12 months.

Our adversaries continue to discover new methods to sabotage, disrupt, or otherwise degrade our systems and extract DoD information. It is critical that DoD components remain vigilant in managing supply chain risk practices when procuring and integrating information and communications technology, whether as a product or as a service, into DoD national security systems.

Attachment:
As stated

---

1 These authorities were initially provided in section 806 of the National Defense Authorization Act for FY 2011.
1. **Trusted Systems and Networks (TSN).** DoD Instruction (DoDI) 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,” outlines a risk management approach that spans the entire system life cycle, including criticality analyses to identify critical functions and components; use of all-source intelligence on suppliers of critical components; and use of TSN processes, tools, and techniques to manage risk.

   a. Per DoDI 5200.44, all DoD national security systems (NSS), including information systems and weapon systems, or systems that have a “high” rating in any of the system categorization security objectives, are required to implement TSN processes to address supply chain risk.

   b. For more information on these processes, see the DoDI 5200.44, DoD Chief Information Officer (CIO) Memorandum, “Guidance for the Procurement and Integration of Information and Communications Technology Components into Critical Information Systems and Networks,” March 24, 2016, and the Defense Acquisition Guide, Chapter 9, “Program Protection.”

2. **NSS Supply Chain Risk Management Authorities.** Section 2339a of title 10, United States Code (“Section 2339a”) authorizes certain DoD officials to take specific procurement actions to mitigate against supply chain risk in the procurement of information and communications technology (ICT) for NSS. These authorities and procedures are implemented at Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 239.73, “Requirements for Information Relating to Supply Chain Risk.” Section 2339a and the implementing DFARS procedures are—

   a. Structured with important safeguards, checks, and balances, such as requiring multiple findings, determinations, and concurrences by specified senior DoD officials (with strict limits on redelegation), and requiring congressional notification when the authority is used; and

   b. Available for use in individual procurements as well as on a “class” basis, where the findings and determinations are applicable to and available for any eligible DoD procurement transaction that is within the scope of the class established in the determination.

3. **Procedures for Enterprise Use of Section 2339a.** To implement statutory NSS supply chain risk authorities and supplement DoD policies and guidance for TSN and Program Protection, the DoD CIO and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) shall execute the following supply chain risk management (SCRM) processes to ensure ICT suppliers or products that represent a “critical” or “high” (or selected “medium”) counterintelligence risk are addressed at the DoD enterprise level.
a. Delegation of Authority and Assignment of Responsibilities. Section 2339a and DFARS subpart 239.73 assign responsibilities and delegate certain authority to the USD(A&S).

1) Pursuant to DFARS 239.7303(b)(1), the USD(A&S) is delegated the authority of the Secretary of Defense to make determinations pursuant to DFARS 239.7304(b), and to take actions authorized by DFARS 239.7305, for any organizational unit of the Department of Defense, including the Military Departments (MILDEPs), and the DoD Fourth Estate (i.e., OSD, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD that are not in the MILDEPs) (collectively “DoD Components”), and any such determination shall be binding on the DoD Component(s) concerned. This authority of the USD(A&S) is distinct from the authority of the Secretaries of the MILDEPs described in paragraph 3.f. and cannot be further redelegated.

2) The remainder of the authorities and responsibilities provided in Section 2339a and DFARS Subpart 239.73 are assigned in the manner set forth in this memorandum.

b. DFARS Clauses. DoD Components shall not purchase ICT for NSS, except through contract vehicles that include the clause at DFARS 252.239-7018, Supply Chain Risk. DoD Components shall include this clause and appropriate provisions, as prescribed at DFARS 239.7306, to enable use of authorities in Section 2339a.

c. Notice of Certain Threat Assessments. The Director, Defense Intelligence Agency (DIA) will notify the DoD CIO, the USD for Research and Engineering (USD(R&E)), the USD(A&S), the Secretaries of the MILDEPS, the Commander, U.S. Cyber Command (CDRUSCYBERCOM), and the Director, Defense Security Cooperation Agency when a “critical” or “high” threat rating on a supplier threat assessment has been completed, as well as when selected “medium” threats have been identified in accordance with established criteria.

d. Assessment of Supply Chain Risk and Scoping of Mitigation Actions. The DoD CIO, the USD(R&E), the USD(A&S), and the CDRUSCYBERCOM, in coordination with the MILDEPs, will—

1) Through the actions of the SCRM Scoping and Mitigations Working Group, assess each of the supplier threat assessments provided by the DIA or other Defense Intelligence Components and determine whether there is significant supply chain risk for DoD NSS; and

2) Document a Scoping and Mitigation decision for all cases in which the use of Section 2339a authority may be warranted, which decision shall—
i. Indicate whether the assessment and determination of risk applies only to an individual procurement transaction (e.g., a unique scenario that is unlikely to occur repeatedly across the enterprise), or applies to a class of procurements (i.e., any procurement that meets the class criteria specified in the scoping decision); and

ii. Recommend specific risk mitigation actions, such as use of the Section 2339a authority to block procurement of the relevant ICT in any DoD NSS, or leaving full discretion regarding the application of the Section 2339a authority with the appropriate, authorized, DoD officials (see DFARS 239.7303 and 239.7304).

e. **Documenting the Joint Recommendation, Concurrence, and Determination to Use Section 2339a Authorities.** For risks requiring action under Section 2339a—

1) The DoD CIO, in coordination with the USD for Intelligence and Security (USD(I&S)) and the USD(A&S), will prepare and execute an action package that contains the Joint Recommendation of the DoD CIO and the USD(A&S), on the basis of a risk assessment by the USD(I&S) (i.e., the DIA threat assessment referenced in paragraph 3.c.), regarding the assessment of significant supply chain risk, and the scope of applicability and the required or recommended mitigations as identified and documented pursuant to paragraph 3.d. (which satisfies the requirements of DFARS 239.7304(a));

2) The action package referenced in e.1), above, may also contain—

   i. The advance concurrence of the USD(A&S) (including any conditions or limitations thereon) for any subsequent Determination by an Authorized Official in a Military Department (see DFARS 239.7303) to exercise the Section 2339a authority for a procurement that is within the scope of the Joint Recommendation, pursuant to DFARS 239.7304(b); and

   ii. The Determination by the USD(A&S) (including any conditions or limitations thereon) to exercise Section 2339a authority for procurements by any DoD Component (including the MILDEPs and the DoD Fourth Estate) that are within the scope of the Joint Recommendation, pursuant to DFARS 239.7304(b).

3) The signed Joint Recommendation, Concurrence, and Determination package will be retained by the DoD CIO, in accordance with applicable recordkeeping guidelines; and

4) Authorized officials will send a notice of the Section 2339a Determination to Congress, as discussed further in paragraph 3.i.

f. **Section 2339a Determinations for the MILDEPs.** After completion of the Joint Recommendation and Concurrence (when the Determination by the USD(A&S) does not
cover the MILDEPs), the Authorized Officials for the MILDEPS (i.e., the Secretaries of the MILDEPs, or their senior acquisition executives if delegated authority pursuant to DFARS 239.7303(b)(2)), shall make the Determination required by DFARS 239.7304(b) and ensure that appropriate notice is provided to Congress (see paragraph 3.j), prior to taking any covered procurement action authorized by DFARS 239.7305. Such Determination(s) to use Section 2339a within a MILDEP may be made for individual procurements, or as a Class Determination for that MILDEP.

g. **Acquisition Workforce Procedures.** To implement Section 2339a Class Determinations made pursuant to paragraphs 3.e. and 3.f., DoD Acquisition personnel shall follow the appropriate acquisition workforce implementation procedures maintained by the Director for Defense Pricing and Contracting (DPC) and available at https://www.acq.osd.mil/dpap/pdi/cyber/enhanced_procedures_for_supply_chain_risk_management.html

h. **Implementing and Documenting the Use of Section 2339a Authorities.** All DoD Components shall implement and document the use of Section 2339a authorities pursuant to any Determination made pursuant to DFARS 239.7304:

1) Withholding information. Section 2339a and DFARS 239.7305(d)) provide authority to limit disclosure of information relating to the basis for a Section 2339a Determination.

2) Notice and opportunity for reconsideration. Section 2339a DoD Authorized Officials shall ensure that each affected entity of each Determination, class or otherwise, is provided the following:
   i. Notice of the issuance of the Section 2339a Determination, including a description of scope;
   ii. The opportunity to request reconsideration of the Determination, which request shall be received no later than 30 days after issuance such notice; and
   iii. A description of the procedures governing such a reconsideration request.

3) Review. Determinations made pursuant to DFARS 239.7304(b) shall be reviewed as needed based on changes to known threat information or other relevant circumstances.

4) Covered Procurement Actions. The Component’s Procurement Executive shall ensure that all necessary covered procurement actions (DFARS 239.7305) are taken and appropriately reported, including—
i. Ensuring that contracts are not awarded, and that consent to subcontract is withheld, for suppliers or products covered by any Determination, except as provided in paragraph h.5); and

ii. Reporting to Defense Pricing and Contracting all Section 2339a covered procurement actions that are within the scope of any Determination, for inclusion in required reports, as described in paragraph j.3).

5) Exceptions to Covered Procurement Actions. The Component Acquisition Executive will identify and report all circumstances for which a covered procurement action that is otherwise required by a Class Determination should not be taken (e.g., mission impact resulting from excluding the entity or product presents a greater risk to national security than the supply chain risk; a technical mitigation or other less intrusive measure is reasonably available to reduce the supply chain risk). The Component shall submit to the Authorized Official a request for exception that includes a detailed description of the circumstances and specific action being proposed that varies from the requirements of the Determination, and how these circumstances and actions effectively address the risk to national security that is described in the Determination. The Component shall not proceed with the proposed activity unless authorized to do so in writing by the Authorized Official that made the determination.

i. Procedures for Notifying Congress of the Use of Section 2339a Authorities. The notice to Congress required by DFARS 239.7304(c) will be accomplished as follows:

1) Section 2339a Class Determinations. For any Class Determination, the Authorized Official making that determination will—
   i. Provide notice to Congress of the initial Class Determination; and
   ii. Report to the DPC for inclusion in the annual report to Congress as described in paragraph 3)—
      1. The initial Class Determination; and
      2. All covered procurement actions made under any such Class Determination(s).

2) Individual Procurements Not Covered by a Class Determination. For a Determination to use Section 2339a for an individual procurement that is not covered by a Class Determination, the Authorized Official making the determination will provide the required notice(s) to Congress, and will report that Determination to the DPC for inclusion in the annual report to Congress as described in paragraph 3).

3) Annual Report. The USD(A&S) shall submit an aggregated report to Congress identifying all covered procurement actions taken by any DoD Component during the reporting period. The report shall be submitted biennially, or as directed by the USD(A&S).
j. **Department of Defense Information Network Operations, Security and Monitoring.**

These procedures in no way limit or alter the authority of the CDRUSCYBERCOM to take all necessary and appropriate action to secure, defend, and operate the DoD Information Network (DoDIN) in accordance with existing authorities. The CDRUSCYBERCOM, in coordination with the Director, National Security Agency, may independently conduct operational and technical observations and assessments to be considered in the scoping and mitigation process outlined above. The CDRUSCYBERCOM will periodically monitor the DoDIN for prohibited hardware, software, or services identified through the processes in this memorandum.