



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 13 2018

MEMORANDUM FOR SECRETARIES OF MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT
DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Enhanced Section 806 Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Networks

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 are extra vigilant in managing supply chain risk practices when procuring and integrating information and communications technology (ICT), whether as a product or as a service, into DoD national security systems (NSS). These activities are vital for protecting the systems and integrity of information relied upon by our warfighters.

DoD is enhancing its procedures to proactively address supply chain threats that present counterintelligence risk to our enterprise, utilizing authorities in section 806 of the Ike Skelton National Defense Authorization Act for FY 2011 (Public Law 111-383), as amended. These procedures ensure that enterprise risk is assessed and mitigated in a timely manner and future procurements of the risky products are blocked when necessary.

The attached document provides details of these new procedures, roles, and responsibilities, which are effective immediately for all DoD Components acquiring or



OSD002982-18/CMD003775-18

sustaining DoD NSS. These changes will be integrated into an update to DoD Instruction 5200.44 in the next 12 months.

Pat M. Sh L

Attachment:
As stated

ENHANCED PROCEDURES FOR ENTERPRISE-WIDE USE OF SECTION 806 SUPPLY CHAIN RISK MANAGEMENT AUTHORITIES FOR DOD NATIONAL SECURITY SYSTEMS

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. **Section 806 Supply Chain Risk Management Authorities.** Section 806 of the Ike Skelton National Defense Authorization Act (NDAA) for FY 2011 (Public Law 111-383), as amended (section 806), authorizes certain DoD officials to take specific procurement actions to mitigate against supply chain risk in the procurement of 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 806 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. **Enhanced Procedures for Enterprise Use of section 806.** To supplement existing TSN, Program Protection, and section 806 policies and guidance, an enhanced enterprise supply chain risk management (SCRM) procedure will be established. The DoD CIO and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) will immediately implement the following process 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 806 and the DFARS assign responsibilities, and allow delegation of authority, to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), which are hereby transferred or redelegated in view of the transition of USD(AT&L) to the new offices of the USD for Research and Engineering (R&E) and USD(A&S) (pursuant to section 901 of the NDAA for FY2017, as amended, and codified at 10 U.S.C. 133a & 133b), as follows:
- 1) Pursuant to DFARS 239.7303(b)(1), the USD(A&S) is hereby delegated the authority of the Secretary of Defense to make determinations pursuant to DFARS 239.7304(b), and to take actions authorized by 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 that are provided for USD(AT&L) in section 806, and the current version of the implementing DFARS Subpart 239.73, are transferred to the USD(R&E) and the USD(A&S) in the manner set forth in this memorandum.
- b. **DFARS Clauses.** Effective immediately, DoD Components will not purchase ICT for NSS except through contract vehicles that include the clause at DFARS 252.239-7018, Supply Chain Risk. DoD Components will immediately take steps to include this clause and appropriate provisions to enable use of authorities in section 806, as prescribed at DFARS 239.7306.
- c. **Notice of Certain Threat Assessments.** The Director, Defense Intelligence Agency (DIA) will notify DoD CIO, USD(R&E), USD(A&S), the Secretaries of the MILDEPs, Commander, U.S. Cyber Command (CDRUSCYBERCOM), and the Director, Defense Security Service (DIRDSS) when a "critical" or "high" threat rating on a supplier threat assessment has been completed, as well as when selected "medium" threat assessments have been identified in accordance with criteria to be established by DoD CIO, USD(R&E), USD(A&S), the Secretaries of the MILDEPs, CDRUSCYBERCOM, and DIRDSS within 30 days of the date of this memorandum.
- d. **Assessment of Supply Chain Risk and Scoping of Mitigation Actions.** The DoD CIO, USD(R&E), USD(A&S), and CDRUSCYBERCOM, in coordination with the MILDEPs, will:

- 1) Assess each of the supplier threat assessments provided by DIA 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 806 authority is 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. Direct or recommend specific risk mitigation actions, such as use of the section 806 authority to block all procurement of the relevant ICT in any DoD NSS, or leaving full discretion regarding the application of the section 806 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 806 Authorities. For suppliers or products requiring action under section 806—

- 1) The DoD CIO, in coordination with the Under Secretary of Defense for Intelligence (USD(I)) and USD(A&S), will prepare and execute an action package that contains the Joint Recommendation of the DoD CIO and USD(A&S), on the basis of a risk assessment by USD(I) (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 1), immediately above may also contain:
 - i. The advance Concurrence of 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 806 authority for a procurement that is within the scope of the Joint Recommendation, pursuant to DFARS 239.7304(b); and
 - ii. The Determination by USD(A&S) (including any conditions or limitations thereon) to exercise section 806 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 stored by DoD CIO; and

- 4) USD(A&S) will send a notice of the section 806 Determination to Congress, as discussed further at paragraph 3.j.
- f. **Section 806 Determinations for the MILDEPs.** After completion of the Joint Recommendation and Concurrence (when the Determination by 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)) may 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 806 within a MILDEP may be made for individual procurements, or as a Class Determination for that MILDEP.
- g. **Procedures for Notifying the Acquisition Workforce.** No later than 60 days of the date of this memorandum, the Director for Defense Procurement and Acquisition Policy (DPAP) will develop procedures that document and inform the Acquisition Workforce regarding all section 806 Class Determinations made pursuant to paragraphs e., and f.
- h. **Procedures for Notifying Vendors.** No later than 60 days of the date of this memorandum, DPAP will develop procedures that will limit the disclosure of information relating to the basis for a section 806 Determination (pursuant to sec. 806(d) and DFARS 239.7305(d)) and govern notification of entities within the scope of the Determination. For Class Determinations, This guidance shall require the following:
 - 1) Notification of each affected entity of each Class Determination and the scope of such Determination, including for:
 - i. The initial Determination by any authorized official; and
 - ii. The results of the annual review of each such Determination (pursuant to paragraph k)
 - 2) Provision to the entity an opportunity to challenge the initial Class Determination or annual review not later than 30 days after receipt of any such notice, in accordance with the DPAP specified administrative procedures.
- i. **Implementing and Documenting the Use of section 806 Authorities.** All DoD Components shall implement and document the use of section 806 authorities pursuant to any Determination made pursuant to DFARS 239.7304:
 - 1) 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 i.2); and

- ii. Reporting to DPAP all section 806 covered procurement actions that are within the scope of any Determination, for inclusion in the annual report described in paragraph j.3).
 - 2) **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 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 accordance with procedures to be developed by USD(A&S) and DoD CIO within 60 days of the date of this memorandum.
- j. **Procedures for Notifying Congress of the Use of section 806 Authorities.** The notice to Congress that is required by DFARS 239.7304(c) will be accomplished as follows:
- 1) **Section 806 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 DPAP 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 806 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 DPAP for inclusion in the annual report to Congress as described in paragraph 3).
 - 3) **Annual Report.** USD(A&S) shall submit an annual, aggregated report to Congress identifying all covered procurement actions taken by any DoD Component during the annual reporting period.
- k. **Annual Review.** All Determinations made pursuant to DFARS 239.7304(b) shall be reviewed annually.

1. **DODIN Operations, Security and Monitoring.** These procedures in no way limit or alter the authority of CDRUSCYBERCOM to take all necessary and appropriate action to secure, defend, and operate the DoD Information Network (DODIN) in accordance with existing authorities. 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. CDRUSCYBERCOM will periodically monitor the DODIN for prohibited hardware, software, or services identified through the processes in this memorandum.