Department of Energy
Acquisition Regulation

No. AL-2021-06
Date September 1, 2021
Amended: October 26, 2022

ACQUISITION LETTER

This Acquisition Letter is issued under the authority of the Senior Procurement Executives of DOE and NNSA. It is intended for use by procurement professions of DOE and NNSA, primarily Contracting Officers, and other officials of DOE and NNSA that are involved in the acquisition process. Other parties are welcome to its information, but definitive interpretations of its effect on contracts, and related procedures, if any, may only be made by DOE and NNSA Contracting Officers.

Subject: Chief Information Officer's Supply Chain Risk Management Program

References:

Federal Acquisition Supply Chain Security Act of 2018,
(Pub. L. 115–390)
Authorities Relating to Mitigating Supply Chain Risks in the Procurement of Covered Articles (41 U.S. Code § 4713)
Enhanced Procurement Authority to Manage Supply Chain Risk (50 U.S. Code § 2786)
FAR 9.104 -- Standards
FAR 9.2 -- Qualifications Requirements
FAR 8.405-1 -- Ordering procedures for supplies, and services not requiring a statement of work.
FAR 8.405-2 -- Ordering procedures for services requiring a statement of work.
FAR 12.603 -- Streamlined solicitation for commercial items
FAR 13.106 -- Soliciting competition, evaluation of quotations or offers, award and documentation.
FAR 15.3 -- Source Selection
FAR 16.505 -- Ordering [under Indefinite-Delivery Contracts].
FAR 17.2 -- Options
FAR 44.2 -- Consent to Subcontracts
FAR 44.3 -- Contractors' Purchasing Systems Reviews

When is this Acquisition Letter (AL) effective?

This Acquisition Letter (AL) is effective immediately upon issuance.

When does this AL expire?

This AL remains in effect until superseded or canceled.

Who is the intended audience for this AL?

Contracting Officers (COs) within the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA).

Who are the points of contact?

For DOE Contracting Officers, contact MA-611, DOE_oapmpolicy@hq.doe.gov.
For NNSA Contracting Officers, contact Ariane S. Kaminsky, Ariane.Kaminsky@nnsa.doe.gov and Drake Russell. Drake.Russell@nnsa.doe.gov .

For additional information on ALs and other issues, visit our website at: http://energy.gov/management/office-management/operational-management/procurement-and-acquisition

What is the purpose of this AL?

The purpose of the AL is to provide guidance to DOE/NNSA Contracting Officer's (COs) on the use of the Chief Information Officer's (CIO) Supply Chain Risk Management Program (OCIO SCRM Program) in conducting Supply Chain Risk Management (SCRM) for Information and Communication Technology (ICT) related procurements. The OCIO SCRM Program is one aspect of an overall SCRM program intended to support the CO in their responsibility not to procure ICT end items determined to have an unacceptable risk to DOE/NNSA.

What types of M&O and non-M&O contracts are affected by this AL?

All contracts, including M&O contracts, and in particular, contracts that include the acquisition of ICT. The OCIO SCRM Program may be useful and should be considered for use in other sensitive procurements including for such items as Bulk Electric System (BES) components, facility and utility system automation and control systems and other Operational Technology (OT) systems, security and surveillance systems, and other at-risk items.

What is the background information?

Executive Order (EO) 14017, *America's Supply Chains,* states that: "The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security." EO 14017 seeks to revitalize and rebuild critical domestic manufacturing capacity, and ensure the availability and integrity of critical goods, products, and services. The need for scrutiny of supply chain risk was highlighted during the 2020 cybersecurity breach where several federal government Information Technology (IT) systems were compromised by foreign adversaries. Initial reports believe that foreign adversaries exploited vulnerabilities in the supply chain of several widely used ICT products. Although supply chain management practices are well engrained in federal acquisition policy and procedures, certain products and services require enhanced scrutiny due to significant inherent risks associated with their supply chain. Recent legislation and executive actions[1] have also increased the necessity for enhanced scrutiny in the acquisition of ICT and BES. These products and their suppliers may have risks in their supply chain that have adverse impacts on: the confidentiality, integrity, and/or availability of systems and services; departmental operations, assets, and individuals; and economic and national security. In the acquisition of ICT, BES, and other sensitive items, COs should make informed risk-based decisions by assessing supply chain risks through multiple risk lenses, such as: national security, cybersecurity, compliance, and finance.

[1] For example, EO 14017: *America's Supply Chains,* EO 14028: *Improving the Nation's Cybersecurity*, and EO 13920: *Securing the United States Bulk-Power System*

Recognizing the need for extra scrutiny of certain supply chains, enhanced procurement authorities have been granted to the Secretary of Energy. The following is a description of the enhanced procurement authorities that the department may use.

Enhanced Procurement Authority for Information and Communication Technology.

The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), enacted under 41 U.S.C. 4713, provides the Secretary of Energy with an enhanced procurement authority. FASCSA provides a mechanism for managing supply chain risk in certain circumstances by permitting the exclusion of contractors, or subcontractors, that pose a supply chain risk. Use of this authority is tantamount to a national security finding. Thus, for Headquarters Procurement Operation procurements, it is recommended that this authority only be used in consultation with the concurrence of the Assistant General Counsel for International and National Security Programs. For field procurements, it is recommended that this authority be used in consultation with the concurrence of the Chief Counsel with cognizance over the procurement. For NNSA it is recommended that the authority only be used in consultation with NNSA Counsel.

Enhanced Procurement Authority for National Security Systems, Nuclear Weapons Components, and Associated Items.

The National Defense Authorization Act for Fiscal Year 2014, codified at 50 U.S.C. 2786, provides the Secretary of Energy with an enhanced procurement authority in the acquisition of certain covered systems[2] and covered items of supply related to national security, not necessarily information technology related. This enhanced procurement authority provides a mechanism for managing supply chain risk in certain circumstances by permitting the exclusion of contractors, or subcontractors, that pose an unacceptable supply chain risk. Use of this authority is tantamount to a national security finding. Thus, for Headquarters Procurement Operation procurements, it is recommended that this authority only be used in consultation/with the concurrence of the Assistant General Counsel for International and National Security Programs. For field procurements, it is recommended that this authority be used in consultation with the concurrence of the Chief Counsel with cognizance over the procurement. For NNSA it is recommended that the authority only be used in consultation with NNSA Counsel.

> Note: The National Defense Authorization Act (NDAA) for Fiscal Year 2021 (Sec. 3161) recently made significant changes to the enhanced procurement authority by the addition of *Special Exclusion Actions*. A *Special Exclusion Action* is an action to prohibit, for a period not to exceed two years, the award of any contracts or subcontracts by the Administration or any other component of the Department of Energy related to any covered system to a source the Secretary determines to represent a supply chain risk. In addition, the 2021 NDAA (Sec. 3161) provides the Secretary the ability to delegate his or her authorities under 50 U.S.C. 2786 to the NNSA Administrator and/or Senior Procurement Executive of the Department. As of the date of this AL, the changes have yet to be codified at 50 U.S.C. 2786.

[2] Covered systems include: National security systems (as defined in section 3552(b) of title 44) and components of such systems; nuclear weapons and components of nuclear weapons; items associated with the design, development, production, and maintenance of nuclear weapons or components of nuclear weapons; items associated with the surveillance of the nuclear weapon stockpile. Items associated with the design and development of nonproliferation and counter proliferation programs and systems. 50 U.S.C. 2786 (f)(5).

Supply Chain Risk Management Program

The DOE's Office of the CIO (OCIO) has deployed a SCRM program to assist COs, program evaluators, and contractors in making risk-informed ICT & BES procurement decisions throughout the procurement lifecycle. COs may consider use of the OCIO SCRM Program for other sensitive procurements as applicable. The OCIO SCRM Program is scalable and adaptable to meet the requirements of Departmental Organizations or Elements, but also to meet the changing SCRM laws, regulations, frameworks, and compliance requirements. The OCIO SCRM Program provides the following benefits:

- Promotes informed decisions by leveraging insights on suppliers when procuring services/products.
- Reduces risk by identifying and treating risk across the risk lenses of financial, cybersecurity, foreign interest, geopolitical, and compliance.
- Helps meet Federal requirements including those established by FASCSA, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)[3], National Institute of Standards and Technology (NIST).

The OCIO SCRM Program is enabled and powered by an end-to-end workflow process and technology tool (provided by an OCIO contractor) that is customizable based on a given entity's risk threshold/tolerance levels across the risk lenses. The program is built on a risk-based approach in which the greater the risk of a supplier, the more due diligence is conducted. The OCIO SCRM program assesses suppliers, supports remediation of risk, and provides risk posture monitoring of the suppliers. The program's product and/or vendor assessment due diligence provides two types of assessments: *Rapid* and *Deep-Dive*. The *Rapid Assessment* is performed first and provides an inherent likelihood risk score for a product or vendor. The *Deep-Dive Assessment* builds off the inherent likelihood risk score by conducting a more comprehensive due diligence review by leveraging questionnaires that have been developed using the NIST 800-161[4] NIST 800-53 r5[5] control family frameworks and provenance guidelines to arrive at a residual risk score. Through these assessments, COs, contractors, and program evaluators can gain valuable insights to assist in their risk-based decisions to procure or not procure a product or service from a given vendor.

What is the guidance contained in this AL?

In the acquisition of supplies or services with significant supply chain risks, a CO should use a SCRM program to assess the level of risk.

[3] North American Electric Reliability Corporation Critical Infrastructure Protection
[4] NIST 800-161: NIST guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks.
[5] NIST 800-53 r5: NIST recommended security controls for federal information systems and organizations.

COs have the option to use the OCIO SCRM Program, or any functionally equivalent SCRM program[6]; however, the OCIO SCRM Program is the preferred program for the acquisition of ICT and BES. Information from the SCRM program should be used in risk-based decisions during the acquisition life cycle, including:

- Subcontractor Consent/Approval
- Contractor Purchasing System(s) Approval
- Exercising of Options
- Exercising an enhanced procurement authority for National Security Systems, Nuclear Weapons Components, and Associated Item under 50 U.S.C.2786.
- Exercising an enhanced procurement authority under 41 U.S.C. 4713.

To access the OCIO SCRM Program, COs can send an email to the DOE SCRM team (doe.scrm@hq.doe.gov). Once the email is received, a DOE SCRM team member will reach out to initiate the onboarding process including process and technology (tool) training.

Use Cases

The following list is not all inclusive but contains cases where a CO should employ a SCRM program prior to making an acquisition decision.

- Contractor Qualifications and Responsibility. Information obtained through a SCRM program may be used in determining whether prospective contractor(s), or subcontractor(s), are responsible under FAR part 9 procedures, specifically, in the application of the procedures at: FAR 9.104, Standards; FAR 9.2, Qualifications Requirements; and FAR 9.3, First Article Testing and Approval.
- Evaluating Proposals and Quotes for Award of a prime contract under FAR Part 15. The CO should not use or require use of the SCRM program as part of or in conjunction with a solicitation evaluation criterion for award of a federal prime contract under FAR Part 15, because doing so, in conjunction with permitting an offeror to correct or explain a supply chain risk after receipt of proposals, could invoke the need to have discussions or raise concerns of unequal treatment.
- Exercising of Option. COs may use the information obtained through a SCRM program in exercising an option(s) at FAR 17.2. If planning to use a SCRM program in post-award supply chain risk management, COs shall include the clause at DOE-H- 20XX, Mitigating Supply Chain Risk in solicitations and contracts.
- Contractor Purchasing System(s) Approval. Contracts may require contractors to use a SCRM program in their purchasing systems and apply it to the contractor's evaluation of subcontracts for products or services that have appreciable supply chain risk. Contractors shall initiate OCIO SCRM Program through their CO.

[6] The characteristics of an equivalent SCRM program would depend largely on the industry standards of the product or service being procured and evaluate risk across the risk lenses of financial, cybersecurity, foreign interest, geopolitical, and compliance.

- Subcontractor Consent. COs may use SCRM program information in providing subcontract consent as applied at FAR 44.2. COs should require subcontract consent, regardless of an approved purchasing system, for products or services where an appreciable supply chain risk exists. COs shall identify the type of products or services that will require subcontract consent at FAR 52.244-2(d) and at clause DOE-H-2058, Designation and Consent of Major or Critical Subcontracts – Alternate I. COs shall include clause at DOE-H-20XX, Mitigating Supply Chain Risk, if the CO anticipates the application of SCRM program information in subcontract review and consent. If the CO reasonably anticipates using Enhanced Procurement Authority for ICT (41 U.S.C. 4713) in subcontract consent, the CO shall include DOE-H-20XX, Mitigating Supply Chain Risk Using Enhanced Procurement Authority for Information and Communication Technology, in solicitations and contracts. If the CO reasonably anticipates using Enhanced Procurement Authority for National Security Systems, Nuclear Weapons Components and Associated Item (50 U.S.C.2786) in subcontract review and consent, the CO shall include clause DOE-H-20XX, Mitigating Supply Chain Risk Using Enhanced Procurement Authority for National Security Systems, Nuclear Weapons Components and Associated Items, in solicitations and contracts.

Attachment – Solicitation Provisions and Contract Clauses

Prescription: Contracting Officers shall insert this clause in solicitations and contracts when using information obtained from a Supply Chain Risk Management (SCRM) program in post-award SCRM.

DOE-H-20XX MITIGATING SUPPLY CHAIN RISK [DATE]

DOE/NNSA utilizes a Supply Chain Risk Management (SCRM) Program to identify, assess, and monitor supply chain risks of critical vendors. The Government may use any information, public and non-public, including all-source intelligence for its analysis. The Contractor agrees that the Government may, at its own discretion, perform audits of supply chain risk processes or events consistent with other terms in the contract regarding access to records and audits. An onsite assessment may be required. Through the information obtained from a SCRM program, DOE may assess vendors and products through multiple risk lenses such as national security, cybersecurity, compliance, and finance. If supply chain risks are identified and corrective action becomes necessary, mutually agreeable corrective actions will be sought based upon specific identified risks. Failure to resolve any identified risk may result in contract termination.

End of Clause.

Prescription: Contracting Officers shall insert this clause in solicitations and contracts, when applicable, to notify contractors that the Government may use Enhanced Procurement Authority for ICT under 41 U.S.C. 4713 to manage supply chain risk.

DOE-H-20XX MITIGATING SUPPLY CHAIN RISK USING ENHANCED PROCUREMENT AUTHORITY FOR INFORMATION AND COMMUNICATION TECHNOLOGY [DATE]

(a) *Definitions.* As used in this clause–

Covered article - The term "covered article" includes-

(1) "Information technology" which means –

(i) any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use-.

(A) of that equipment, or

(B) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(ii) computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; however,

(iii) does not include any equipment acquired by a federal contractor incidental to a federal contract.

(2) "Telecommunications Equipment", which means equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades).

(3) "Telecommunications Service", which means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

(4) the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or

(5) hardware, systems, devices, software, or services that include embedded or incidental information technology.

Supply Chain Risk- The term "Supply Chain Risk" means the risk that a person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

(b) The Contractor shall take all prudent actions, and comply with all Government directions (as identified in (c)), to mitigate supply chain risk when providing covered articles or services affecting covered articles to the Government.

(c) In order to manage supply chain risk, the Government may use the authority provided by 41 U.S.C. 4713 to, among other things, withhold consent for the Contractor to subcontract with a particular source or direct the Contractor to exclude a particular source from consideration for a subcontract under the contract.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

End of Clause.

Prescription: Contracting Officers shall insert this clause in solicitations and contracts, when applicable, to notify the Government that it may use Enhanced Procurement Authority for National Security Systems, Nuclear Weapons Components and Associated Items under 50 U.S.C. 2786 to manage supply chain risk.

DOE-H-20XX MITIGATING SUPPLY CHAIN RISK USING ENHANCED PROCUREMENT AUTHORITY FOR NATIONAL SECURITY SYSTEMS, NUCLEAR WEAPONS COMPONENTS AND ASSOCIATED ITEM [DATE]

(a) *Definitions.* As used in this clause–

(1) "Covered system" means-

(A) National security systems (as defined at 44 U.S. Code § 3552) and components of such systems;

(B) Nuclear weapons and components of nuclear weapons;

(C) Items associated with the design, development, production, and maintenance of nuclear weapons or components of nuclear weapons;

(D) Items associated with the surveillance of the nuclear weapon stockpile; or

(E) Items associated with the design and development of nonproliferation and counterproliferation programs and systems.

(2) "Covered item of supply" means an item—

(A) that is purchased for inclusion in a covered system; and

(B) the loss of integrity of which could result in a supply chain risk for a covered system.

(3) "Supply Chain Risk" means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system or covered item of supply so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system or item of supply.

(b) The Contractor shall take all prudent actions, and comply with all Government directions (as identified in (c)), to mitigate supply chain risk when providing covered systems or covered items of supply to the Government, and services affecting covered systems or covered items of supply.

(c) In order to manage supply chain risk, the Government may use the authority provided by 50 U.S.C. 2786, to, among other things, withhold of consent for the Contractor to subcontract with a particular source or direct the Contractor to exclude a particular source from consideration for a subcontract under the contract When the Government exercises this authority, it will only provide the Contractor with information pertaining to the basis of the action to the extent necessary to carry out the action. No action taken by the Government pursuant to 50 U.S.C. § 2786 shall be subject to review in any Federal court.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

End of Clause.