Subchapter 3004.23 Federal Acquisition Security Council

3004.2300 Scope of subpart.

This subchapter establishes policies and procedures for complying with Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (title II of Pub. L. 115-390) exclusion or removal orders and sharing certain supply chain risk information. "FASCSA orders" refers to both exclusion and removal orders.

3004.2302 Sharing supply chain risk information.

(a) *Information sharing*. 41 CFR 201–1.201 requires agencies to share relevant supply chain risk information with the FASC if the agency has determined there is a reasonable basis to conclude a substantial supply chain risk associated with a source or covered article exists.

(1) The DHS Cybersecurity Supply Chain Risk Management (C-SCRM) Office will gather relevant supply chain risk information and submit it through the DHS FASC Liaison to the FASC Information Sharing Agency (ISA). Relevant information includes:

(i) Information associated with a particular source, a covered article, or a covered procurement (as defined at 41 U.S.C. 4713(k));

(ii) Supply chain risk information that the DHS C-SCRM Office determines indicates a substantial supply chain risk associated with a source, a covered article, or a covered procurement; or

(iii) Supply chain risk management information associated with a source, a covered article, or a covered procurement action and DHS C-SCRM Office deems such information relevant to share with the FASC.

(2) The DHS C-SCRM Office will determine whether substantial supply chain risk information identified by the contracting officer, or another acquisition team member will be shared with the FASC.

(b) *Notification Procedures.*

(1) For any discovery or disclosure of actual or potential supply chain risk information, the contracting officer or another acquisition team member must contact the DHS C-SCRM Office by email at cscrm@hq.dhs.gov. The notification to the DHS C-SCRM Office should include:

(i) Contract or solicitation information, including contract or solicitation number, contractor or offeror name, and name of Component contracting officer;

(ii) Covered article or source name; and

(iii) A "critical date," no less than three (3) business days in the future, for when a response from the DHS C-SCRM Office is requested.

(2) The contracting officer or another acquisition team member submitting the notification should:

(i) Immediately notify the DHS C-SCRM Office even if all the information requested or considered to be relevant is not available;

(ii) Exclude source selection sensitive information in the notification to the DHS C-SCRM Office; and

(iii) Exclude other sensitive information (e.g., IP address, access information such as an account login and password) in the notification to the DHS C-SCRM Office. The notification should state that additional information is sensitive and will be provided in person or via a secured method.

(3) After initial notification, the DHS C-SCRM Office may request additional information.

3004.2304 Procedures.

(d) *Agency specific procedures.* Most orders issued under FASCSA authorities, hereby referred to as "FASCSA orders," will be searchable within SAM to enable contractors and the Government to more easily identify the products and services subject to the orders. However, in rare cases, FASCSA orders may not be listed in SAM. For example, orders arising from classified contracts may not be listed in SAM. FASCSA orders not entered in SAM will be identified in the solicitation. Contracting officers will learn of these applicable orders from the requiring office or program office directly.

(e) *Disclosures*. The purpose of the disclosure is so the Government may decide whether to pursue a waiver in accordance with the procedures at HSAM 3004.2305. If an offeror cannot represent compliance with the prohibition, then the offeror must disclose proposed use of an excluded product or service pursuant to FAR 52.204-29(e). Upon receipt of disclosure of FASCSA order violations, the contracting officer must follow the procedures at HSAM 3004.2302(b) and consult the program office or requiring office regarding whether to pursue a waiver. Upon receipt of disclosure, the contracting officer may determine that the offeror is not eligible for award and make award to another offeror.

(g) *Reporting.*

(1) *Pre-Award.* Offerors must regularly review SAM for applicable FASCSA orders. By submitting an offer, an offeror is representing that it has conducted a reasonable inquiry and is not providing or using any covered article, or any products or services subject to an applicable FASCSA order identified in the solicitation.

(2) *Post-Award.* Once an award is made, contractors are required to monitor SAM at least once every three months to search for excluded sources, products, and services and notify the contracting officer if new FASCSA orders impact the contractors' supply chains (see FAR 52.204-30 (c)(1)).

(i) After engaging with the program office or requiring office, the contracting officer must follow the procedures at HSAM 3004.2302(b) if a contractor submits a report pursuant to paragraph (c) of FAR clause 52.204-30.

(ii) Contracting officers must then coordinate with the program office or requiring office to decide whether to pursue a waiver. If it is determined that a waiver is to be pursued, the contracting officer must follow the procedures at HSAM 3004.2305(d). If a waiver is not granted or pursued, the contracting officer must follow the procedures at HSAM 3004.2305(d)(2).

3004.2305 Waivers.

(d) *Waiver request packages*.

(1) The contracting officer, coordinating with the program office or requiring office, shall decide whether to pursue a waiver or to make award to an offeror who does not require a waiver in accordance with the procedures at 4.2304(f). If a waiver is being pursued, then the contracting officer may not make an award until written approval is obtained from the Secretary of the Department of Homeland Security, or designee confirming the waiver has been granted.

(2) If a waiver is not granted or pursued and the contractor is not in compliance with applicable FASCSA orders, the contracting officer shall not make an award to that offeror and existing contract, or task/delivery order options may not be extended or renewed. This is considered substantial supply chain risk information and the contracting officer must report to the DHS C-SRCM Office following the procedures at HSAM 3004.2302(b).

(3) If the contracting officer, after engaging with the program office or requiring office, decides to pursue a waiver (partial or full), the contracting officer must submit the necessary information to the program office or requiring office's respective Component CIO and CISO, who will review and evaluate for concurrence or denial. The following information must be provided:

(i) Identification of the applicable FASCSA order;

(ii) A description of the waiver sought, including, if limited to only a portion of the FASCSA order, a description of the FASCSA order provisions from which a waiver is sought;

(iii) The name or a description sufficient to identify the covered article or the product or service provided by a source that is subject to the FASCSA order from which a waiver is sought;

(iv) Compelling justification for why a waiver should be granted, such as the impact of the FASCSA order on the Component's ability to fulfill its mission-critical functions, or considerations related to the national interest, including national security reviews, national security investigations, or national security agreements; and,

(v) Any alternative mitigations to be undertaken to reduce the risks addressed by the FASCSA order.

(4) The contracting officer and program office or requiring office are required to review the disclosure and accompanying information for accuracy and completeness before routing the waiver request package to the program office or requiring office's respective Component CIO and CISO.

(5) If the Component CIO decides to pursue the waiver, the waiver package will be sent to the DHS C-SCRM Office.

(6) The DHS C-SCRM Office will review the waiver package and send to the DHS CISO with any relevant comments.

(7) The DHS CISO will review the waiver request package, in consultation with the other members of the DHS C-SCRM Team (comprised of representatives from OCPO, OCIO, and OCSO) and the relevant Component CIO and CISO that submitted the waiver.

(8) If the DHS CISO concurs with the waiver request, the CISO will send the package to the DHS CIO for review. If the DHS CIO does not concur with the waiver request, the package will be rejected and the relevant Component CIO or CISO will be notified.

(9) If the DHS CIO concurs with the waiver request package, the DHS CIO will recommend the waiver to the Secretary of the Department of Homeland Security, or designee, for review and evaluation.

(10) The DHS Secretary will make a final determination regarding the disposition of the waiver. If the DHS Secretary approves or disapproves the waiver, the DHS CIO, in collaboration with the DHS C-SCRM Office, will notify the Component CIO or CISO of the decision. If the DHS Secretary does not approve the waiver, the notification to the Component CIO or CISO may include a timeline for remediation of any deficiencies.

(11) For waiver request packages to applicable DoD or Office of the Director of National Intelligence (ODNI) FASCSA orders, the Secretary of the Department of Homeland Security, or designee, will submit the waiver request package in writing and coordinate with the respective issuing official for review and evaluation.