Continuous Diagnostics and Mitigation (CDM)
Approved Products List (APL)
Supply Chain Risk Management (SCRM) Plan

The Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Product Submission Instructions reference the requirement to submit a Supply Chain Risk Management Plan (SCRM) as part of that activity. The CDM APL SCRM Plan is in support of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "SA-12" supply chain control. The purpose of this document is to provide background information on the SCRM requirement and outline the instructions an offeror is to follow in completing and submitting the CDM APL SCRM Plan.

The CDM APL SCRM Plan consists of (1) the completed questionnaires (Attachment A – CDM-APL-SCRM), and (2) additional information the offeror wishes to provide.

APL submission packages that do not include completed CDM-APL-SCRM questionnaires will fail conformance. Additional information can be submitted; APL packages will not fail conformance for the lack of providing SCRM information beyond the questionnaires for CDM-APL-SCRM.

1. Instructions

Submit the completed SCRM Plan as part of the CDM APL product submission package. One SCRM Plan shall be submitted by each offeror for each manufacturer if that manufacturer's SCRM practices are consistent across all of the proposed products. If a manufacturer's SCRM practices are not consistent across all of the proposed products, the offeror shall submit a SCRM Plan for each product or product family that has consistent SCRM practices. **At a minimum, offerors shall complete the CDM-APL-SCRM. Offerors are encouraged to provide any other relevant SCRM information that will assist an Agency or ordering activity in making a better informed risk decision when considering or using products from the CDM APL**. The SCRM Plan(s) shall cover all of the items proposed for inclusion on the CDM APL. All items proposed for inclusion in the CDM APL shall be offered by (1) the original manufacturer, or (2) an authorized supplier.[1]

2. Objective

The objective of CDM SCRM Plan is to provide information to Agencies and ordering activities[2] about how the offeror identifies, assesses, and mitigates supply chain risks in order to facilitate better informed decision-making by Agencies and ordering activities. The SCRM Plan is intended to provide visibility into, and improve the buyer's understanding of, how the Offeror's proposed products are developed, integrated and deployed; as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products. As stated in the CDM APL product submission instructions, the SCRM Plan shall be submitted as part of the CDM Approved Product List product submission package. **The offeror's SCRM Plan(s) will be made available to Agencies and ordering activities to facilitate market research and requirements definition for procurements that may include Offeror's product.**

(continue to next page)

[1] "*Authorized supplier*," as used in the CDM program, means a supplier, distributor, or an aftermarket manufacturer with a contractual arrangement with, or the express written authority of, the original manufacturer or current design activity to buy, stock, repackage, sell, or distribute the item.

[2] GSA Order ADM 4800.2I, *Eligibility to Use GSA Sources of Supply and Services*, provides definitive guidelines concerning eligibility requirements and limitations for agencies, activities, and organizations (available at: GSA Order ADM 4800.2I Eligibility to Use GSA Sources of Supply and Services).

3. Authority

Office of Management and Budget Circular A-130: The Office of Management and Budget (OMB) Circular A-130 "*establishes general policy for the…acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services*." The requirements of A-130 "*apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government*." The CDM APL SCRM Plan addresses the specific requirements of A-130 as described below.
The information contained in each Offeror's SCRM Plan allows the CDM PMO and the Agencies to:

- Consider "*supply chain security issues for all resource planning and management activities throughout the system development life cycle;*"
- "[A]*nalyze risks (including supply chain risks) associated with potential contractors and the products and services they provide;*"
- "[A]*llocate risk responsibility between Government and contractor when acquiring IT;*" and
- "[I]*mplement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle*."

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*: The CDM APL SCRM Plan requirements are derived from NIST Special Publication 800-161, which "*provides guidance to federal agencies on managing ICT supply chain risks to their information systems and organizations*." The guidance in SP 800-161 is explicitly "*recommended for use with high-impact systems*." The Security Category of the CDM Program is high-impact,[3] so the guidance in SP 800-161 was used to develop these SCRM Plan requirements.

4. Attachments

Attachment
A-CDM-APL-SCRM.xl

[3] The CDM program FIPS 199 Security Classification is {(confidentiality, HIGH), (integrity, HIGH), (availability, MODERATE)}.