CDM APL: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN BACKGROUND

OVERVIEW

CISA's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies. These technology solutions provide visibility into agency networks and help defend against cyber adversaries. The CDM Program Approved Products List (APL) is the authoritative catalog of cybersecurity products that meet CISA's technical requirements and qualify for use in CDM implementations. CISA lists cyber products and related services on the CDM APL only after they pass a thorough vetting process. Software and hardware manufacturers and resellers can submit products for APL consideration monthly. CISA reviews submissions against defined criteria to validate the offerors' claims that their products meet relevant CDM capability requirements.

ABOUT THE CDM APL SCRM PLAN

Offerors are required to include a completed Supply Chain Risk Management (SCRM) Plan Questionnaire with each CDM APL submission.[1] The text below provides background information on the SCRM requirement.

Objective

The objective of the CDM APL SCRM Plan is to provide information to agencies and ordering activities about how the offeror identifies, assesses, and mitigates supply chain risks to facilitate informed decision-making by agencies and ordering activities.[2] 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
- The processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products

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 the offeror's product.

Components

The CDM APL SCRM Plan consists of two components:

1. **Required:** The completed two-part questionnaire (CDM APL SCRM Plan Questionnaire FY2023), available at CDM Approved Products List
2. **Optional:** Additional information the offeror wishes to provide

APL submission packages that do not include a completed CDM APL SCRM Plan Questionnaire will fail conformance.

- Offerors shall submit a completed SCRM Plan as part of the CDM APL product submission package.
- If a manufacturer's SCRM practices are consistent across the product family, the offeror can submit one SCRM Plan for the manufacturer. If a manufacturer's SCRM practices are not consistent across all of the proposed products, the offeror should submit a CDM APL SCRM Plan for each product or product family with consistent SCRM practices.

---

[1] The CDM APL SCRM Plan supports National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Section SA-12: Supply Chain Protection.
[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).

cisa.gov csd_cb.acqbudg@cisa.dhs.gov

- **At a minimum, offerors shall complete the CDM APL SCRM Plan Questionnaire. They are encouraged to provide any other relevant SCRM information that will assist an agency or ordering activity in making well-informed risk decisions when considering or using products from the CDM APL.**
- The submitted SCRM Plan(s) shall cover all of the items proposed for inclusion in the CDM APL. (All items proposed for inclusion in the CDM APL shall be offered by either the original manufacturer or an authorized supplier.[3])

Authority

Office of Management and Budget (OMB) Circular A-130: 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 an offeror's SCRM Plan allows the CDM Program Management Office 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"
- "Implement 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 SP 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,[4] so the guidance in SP 800-161 was used to develop these SCRM Plan requirements.

[3] "Authorized supplier," as used in the CDM Program, means a supplier, distributor, or an aftermarket manufacturer that has 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.
[4] The CDM Program's Federal Information Processing Standard Publication (FIPS) 199 Security Classification is [(confidentiality, HIGH), (integrity, HIGH), (availability, MODERATE)].