# CDM APL: PRODUCT SUBMISSION INSTRUCTIONS

## BACKGROUND

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.

## CDM APL PRODUCT SUBMISSION INSTRUCTIONS

This section outlines how offerors (vendors or resellers) can submit products for possible inclusion on the CDM APL. CISA will evaluate each submission using the process outlined below. (To request a CDM APL product deletion or modification, see the instructions on page 2.) See also the Instructions tab within the CDM APL Submission Form.

**When to Submit Requests:** CISA accepts requests to add/delete/modify CDM APL content monthly. Offerors can submit requests Monday through Friday of the first *full or partial* week of each month. A submission calendar listing submission periods for each month can be found at CDM Approved Products List.

**How to Submit Requests:** Offerors must submit a separate submission package for each product family.[1] Send submissions to csd_cb.acqbudg@cisa.dhs.gov using the following in the subject line:
CDM APL Submission: Offeror Company, Product Manufacturer, Product Family, Date of Submission (YYYY-MM-DD)

### Additions

**What to Submit:**

1. **CDM APL Submission Form:** A detailed spreadsheet available for download at CDM Approved Products List. Note that this form has four tabs:
    - **Instructions:** information to help offerors fill out the other three tabs
    - **Form:** mandatory form to be filled out
    - **Products:** mandatory product information to be provided
    - **Potential CDM Capabilities:** optional questionnaire for those submitting innovative new products
2. **Supply Chain Risk Management (SCRM) Plan Questionnaire:** An Excel sheet available for download at CDM Approved Products List. This questionnaire has two parts, found in the following tabs:
    - Product Assurance
    - Supplier Management
3. Voluntary Product Accessibility Template (VPAT)**:** A template used to document a product's conformance with accessibility standards and guidelines (available for download at Section508.gov). Offerors should use this template to explain how their information and communication technology (ICT) products (software, hardware, electronic content, and support documentation) meet Section 508 standards.

[1] A product family is a manufacturer's suite of products (with similar capabilities) that comprise a solution. If a product family meets various CDM capability requirements, the offeror should submit a separate CDM APL Submission Form for each CDM capability. Therefore, a given product family might have multiple submission forms reflecting multiple capabilities.

4. **End User License Agreement (EULA):** A legally binding document defining the user's rights and restrictions for using the offeror's products; also known as a commercial supplier agreement.

### Deletions

**What to Submit:**

1. **APL Submission Form:** A spreadsheet available for download at CDM Approved Products List. To request that a product be removed from the CDM APL:
    - **On the Form tab**: Complete rows 4 through 9
    - **On the Products tab:** In the Indicator column, select D (for Delete). In the Manufacturer Part Number (SKU) column, list the SKUs of the products to be deleted.

### Modifications

**What to Submit:**

1. **APL Submission Form:** A spreadsheet available for download at CDM Approved Products List. To request that a product be modified on the CDM APL:
    - **On the Form tab**: Complete rows 4 through 9
    - **On the Products tab:** In the Indicator column, select M (for Modify). Indicate requested changes in the relevant fields. Use bold to call attention to new content.

## CISA'S TECHNICAL EVALUATION

**Part 1: Conformance**

CISA conducts an initial conformance review of each submission package to ensure that:

- CDM APL Submission Form is complete and the offeror has provided all required documentation
- Product has a government or commercial presence
- Product supports Internet Protocol Version 6 (IPv6)[2] or is scheduled to meet IPv6 by the end of FY 2023

If a submission fails the initial conformance review, CISA will notify the offeror and note areas of non-conformance. The offeror can then correct the package and resubmit within the submission period or wait until a future submission period. A failed submission does not undergo technical evaluation.

**Part 2: Self-Certified Common Requirements**

CISA verifies that the offeror has self-certified that the submitted product meets all of the Common Requirements published in CDM Technical Capabilities, Vol. 2 (2021), available for download at CDM Approved Products List. The Common Requirements (requirements common to all CDM capabilities) encompass the following:

1. Actual state
2. Interoperability
3. Scaling
4. Securing
5. Timeliness and completeness
6. Grouping
7. Policy decision point

[2] Per OMB Memorandum M-21-07: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

If an offeror doesn't certify that the submission meets all of the Common Requirements, the submission will be rejected and will not undergo technical evaluation.

### Part 3: Product Meets a Core CDM Capability Functional Requirement

CISA evaluates the offeror's claims against the core CDM capabilities areas published in CDM Technical Capabilities, Vol. 2 (2021):

1. What is on the network? (Asset Management)
2. Who is on the network? (Identity and Access Management)
3. What is happening on the network? (Network Security Management)
4. How is data protected on the network? (Data Protection Management)

Please see the Instructions tab on the CDM APL Submission Form for information about how many capabilities the product must meet within each capabilities area/grouping.

Offerors must complete Column F (Supporting Information) and Column G (Evidence) in the Form tab of the CDM APL Submission Form. In the Supporting Information column, please provide documentation (company website, white paper references, third-party research) that supports your claim that the product meets the capability. In the Evidence column, please explain how the provided supporting information demonstrates that the product meets the capability. See the appendix (page 5) for a more detailed explanation.

### Part 4: Potential CDM Capabilities

Offerors are invited to submit new products for consideration under the Potential CDM Capabilities category. CISA understands that the cybersecurity market is continuously developing at a rapid pace, making previous and current technologies costlier and less effective than new solutions. The CDM Program therefore provides a means to submit new, innovative products for review. The Potential CDM Capabilities category gives offerors the ability to influence future CDM capabilities and present such technologies to CISA for CDM APL consideration.

Products submitted in this category must meet the CDM Common Requirements; however, they may not necessarily map to a core CDM functional capability. These products should show rapid and wide adoption by industry verticals, as well as clear alignment with relevant cybersecurity domains.

Offerors must complete all fields in the Potential CDM Capabilities questionnaire (the fourth tab in the APL Submission form) for the product to undergo a conformance review and technical evaluation.

### Part 5: Next Steps

**If Products Are Accepted:** If CISA finds submitted products to be fully or partially acceptable, the agency notifies the offeror via email, specifying which products have been approved and for what capabilities. Approved products will be added to the APL, which is republished at the beginning of every month at CDM Approved Products List.

CISA also notifies the following partner agencies of the products' acceptance on the APL:

- General Services Administration (GSA): CDM products are available for federal agencies to purchase through GSA's Multiple Award Schedule (MAS) Information Technology contract on GSAAdvantage.gov. GSA tags all approved CDM products on the GSA Advantage site with the CDM symbol.
- National Aeronautics and Space Administration (NASA): CDM products offered by NASA Solution for Enterprise-Wide Procurement (SEWP) contract holders are available for purchase through the NASA SEWP CDM Catalog. The NASA SEWP team will engage with offerors on adding their products to the catalog.

**If Products Are Not Accepted:** If CISA determines that submitted products do not meet the CDM capabilities requirements, the agency notifies the offeror via email, identifying areas of non-acceptance. The offeror has the option of modifying the package and resubmitting it in the future.

## CONTACT

If you have questions or comments, please send an email to the CDM Program Management Office in the Acquisition and Budget Branch at csd_cb.acqbudg@cisa.dhs.gov.

# APPENDIX: EVIDENCE EXAMPLES

The CDM APL Submission Form asks offerors to provide supporting information (Column F) and evidence (Column G) for each product submitted for CDM APL consideration. Following are examples for two specific CDM requirements.

## Req. CMN 7-1

This requirement addresses the question of how the product can be scaled to accommodate data growth. The intent is to enable customers to plan for current and future capacity needs.

1. **Supporting Information:** Give a detailed technical explanation of how the product (SKU ID) meets the requirement.

   Example: "A quantity of X products (SKU ID) would be required to support Y gigabytes of network traffic. For each gigabyte of network traffic generated, Z additional products (SKU ID) would be required."

2. **Evidence:** Provide online resources or attached documents (such as a formal sizing/capacity guide) with a specific section or page referenced. If you reference a sizing guide, please include it with submission documents.

   Example: "Please see page 1.2 of Attachment X and page 3.1 of Attachment Y for evidence that the submitted product meets the scale requirements."

## Req. EDR 1-3

This requirement addresses how the Endpoint Detection and Response (EDR) capability shall configure an agency's policy to implement a response action on an endpoint device. This policy is related to the Policy Enforcement Point (PEP) for remediation (incident response based on configured endpoint response actions). Note that agency policy could be to implement no automatic response actions.

1. **Supporting Information:** Explain how the product provides an online central management console where response policies and incident workflows can be created, configured and deployed. An endpoint response policy (to isolate the endpoint from the network, or to quarantine executables) can be created using the console.

   Example: "Click on the Menu tab and the 'Create response policy' button. Screenshot is attached to this submission." (Attach a screenshot of management console showing configuration of response action.)

2. **Evidence:** Provide an attached document or online resource with the specific section or page referenced.

   Example: "Supporting information is found in Section 1.2.1 of the referenced document. Creating an incident workflow is described in Section 1.2.3 of the document." (Provide a URL or attach the documentation.)