

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Product Submission Instructions

This document outlines how vendors can submit products to DHS for consideration to be added, deleted, and or modified on the CDM APL and how DHS will evaluate each submission.

Submissions

When to Submit: DHS accepts submissions to add to/delete from/modify the CDM APL monthly. Offerors can submit changes to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on our website.*

How to Submit: Offerors must submit a separate package for review for each Product Family¹. Submissions should be sent to csd_cb.acqbudg@cisa.dhs.gov using the following subject line: CDM APL Submission: Company, ProductManufacturer, ProductFamily, DateofSubmission (YYYY-MM-DD).

What to Submit:

- **APL Submission Form***
- **Required Supporting Documentation**
 - VPATs (to include 508 testing results)
 - Commercial Supplier Agreement Terms
 - Supply Chain Risk Management (SCRM) Plan Questionnaire (Attachment A)*
 - Product Assurance
 - Supplier Management
- **Supporting Documentation-** Any white paper or marketing material that supports your products' claim(s) or list a company website URL on the product submission form that supports the claim.

Evaluations

Part 1: Conformance: DHS will conduct an initial conformance review of the package to ensure:

- The CDM APL Submission Form is complete and the offeror has provided and completed all required supporting documentation
- The products have either a government or commercial presence
- The products currently support Internet Protocol Version 6 (IPv6)² or are scheduled to meet IPv6 by the end of FY2023

If a submission fails the initial conformance, DHS will notify the offeror and provide areas of non-conformance for re-submission. Offeror can re-submit within the submission period, or wait until the following month's submission period. The submission will not be technically evaluated.

Part 2: Common Requirements are Self-Certified: DHS will ensure that the offeror has self-certified that they meet all of the Common Requirements as written in CDM Technical Capabilities Volume 2*, which are:

- 1) Common Actual State
- 2) Common Interoperability
- 3) Common Scaling
- 4) Common Securing
- 5) Common Timeliness and Completeness
- 6) Common Grouping
- 7) Common Policy Decision Point

If an offeror doesn't certify that they meet all of the Common Requirements, their submission will be rejected and the submission will not be technically evaluated.

1. A Product Family is considered a suite of products with the same capabilities that comprise a solution. If products have different capabilities, they should be submitted as separate Product Families.

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

*<https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program>

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Product Submission Instructions

Part 3: Product Meets a Core CDM Capability Functional Requirement: DHS will evaluate offeror's claims against CDM Technical Capabilities Volume 2, which are grouped as follows:

- 1) What is on the Network (Asset Management)
- 2) Who is on the Network (Identity and Access Management)
- 3) What is Happening the Network (Network Security Management)
- 4) How is Data Protected on the Network (Data Protection Management)

Please refer to the Instructions tab on the Submission Form for more information about how many capabilities must be met within each grouping.

Offerors must complete Columns F and G within the Submission Form which asks for Supporting Information and Evidence, respectively. In the Supporting Information column, we are looking for documentation (company website, white paper, third party research) that supports your claim that the product meets the capability. In the Evidence column, we are looking for you to expound on how the provided supporting information demonstrates that the product meets the capability.

Part 4: Potential CDM Capabilities

Offerors have the opportunity to submit products for consideration under the CDM Potential Capabilities category. The CDM program understands that the cybersecurity market is continuously developing at a rapid pace, making previous and present technologies unwieldy, expensive, and ineffective in comparison.

To that end, the program is providing a means to submit new and innovative products for CDM program review. These products should show rapid and wide adoption by industry verticals, as well as a clear understanding of the cybersecurity domains being addressed.

This category gives the offeror the ability to have an impact on future CDM capabilities and provides a means for such technologies to be considered for the CDM APL.

Products submitted in the category must still meet the Common Requirements, however, they do not necessarily map to a core CDM Functional Capability. Offerors must complete the Potential Capabilities Questionnaire that is located in the APL Submission form (Tab 4) in order to submit their application. All fields must be completed in this section in order to pass conformance and be technically evaluated.

Part 5: Next Steps

Products were Accepted: If DHS determines that products were found fully or partially acceptable, we will notify the offeror via email that the products have been approved and for what capabilities. The approved products will be added to the APL, which is republished at the beginning of every month.

DHS also notifies Multiple Award Schedule (MAS) Information Technology of the products' acceptance on the APL in the event that you would like to modify your MAS contract to include the newly accepted products on the CDM Tools Special Item Number (SIN) 541519CDM³. The offeror is responsible for submitting a formal modification request or offer through the e-mod/e-offer system. More information can be found on our website⁴.

Products were Not Accepted: If DHS determines that the products do not meet the CDM capabilities, we will notify the offeror and identify areas of non-acceptance. Offeror can modify their submission and re-submit the following month if they choose to.**

³ GSA is responsible for the final approval to add products to the CDM Tools Special Item Number (SIN) 541519CDM and associated offerings or award offer. This includes Commercial Supplier Terms and Letters of Supply (LOS) if not the original manufacturer, and in accordance with GSA's solicitation requirements.

⁴ <https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program>

**Disclaimer: Products not on the CDM APL will not be added to the CDM Tools Special Item Number (SIN) 541519CDM

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Product Submission Instructions

For any questions or comments- please contact the DHS CDM Program Management Office (PMO),
Acquisition and Budget (AB) for more information at csd_cb.acqbudg@cisa.dhs.gov.