Continuous Diagnostic and Mitigation and Continuous Monitoring as a Service

CMaaS TASK AREAS

CMaaS TASK AREAS

The contractor shall provide functional, strategic, and managerial business consulting and support services in the execution of the overall program missions. Activities to be supported under this BPA by orders are described below:

Unless stated otherwise in the RFQ under this BPA, at the order level, the Government will provide specific requirements regarding the target IT environment for the agency or organization for which CMaaS is required, in sufficient detail that the provider can determine the number and type of assets for which sensors need to be provided and the frequency of data collection (e.g., asset discovery, vulnerability scanning) required by the requesting organization. Subject to specific order requirements, the baseline number of IT assets may be provided based on a preliminary asset inventory conducted by the Government using its own non-commercial discovery tool. The order request will also specify any existing sensor tools, dashboards, or other applications or data sources (i.e., already installed and in operation by the requesting organization) that the CMaaS provider must integrate in its proposed solution architecture, as well as any unique security requirements.

1. Provide Order Project Management Support
2. CDM Order Planning
3. Support CDM Dashboards
4. Provide-Specified Tools & Sensors
5. Configure & Customize Tools & Sensors
6. Maintain Data On Desired State For CDM Tools & Sensors
7. Operate CDM Tools & Sensors
8. Integrate & Maintain Interoperability Between CDM Tools & Agency Legacy Applications & Data
9. Operate Data Feeds To & From Installed Dashboards
10. Training & Consulting In CDM Governance For Departments, Agencies, & Other Requesting Organizations
11. Support Independent Verification & Validation (Iv&V) & System Certification

TASK AREA 1 – PROVIDE ORDER PROJECT MANAGEMENT SUPPORT

The contractor shall provide all necessary personnel, administrative, financial, and managerial resources necessary for the support of order accomplishment. This includes the management and oversight of its performance of the order under the BPA and work performed by contractor personnel, including subcontractors and teaming arrangements/partners, to satisfy the requirements identified in the orders. The contractor should note that adding labor categories is permissible.

The contractor shall provide this support in accordance with the terms and requirements of this BPA and the specific requirements of the order.

Examples of support:

a. Coordinate a Program Kickoff Meeting.

b. Prepare a Monthly Status Report (MSR) at the BPA and order levels.

c. Convene technical status meetings.

d. Prepare project management documentation such as a project management plan (PMP), staffing plan, project schedule, and work breakdown structure (WBS).

e. Manage contractor personnel assigned to the order.

f. Prepare trip reports.

g. Prepare problem notification reports.

h. Notify the Contracting Officer (CO), the Contracting Officer Representative (COR), and Order Government Technical Point of Contact (TPOC) of any technical, financial, personnel, or general managerial problems encountered throughout the BPA and individual orders.

i. Develop and deliver detailed project plans for each order.

j. Evaluate orders under this BPA using Earned Value Management (EVM), where required.

Return To Top

TASK AREA 2 – CDM ORDER PLANNING

The contractor shall provide plans describing their proposed approach to implement the specific CDM capabilities required by the order. The contractor shall also participate in and /or facilitate technical design reviews consistent with agency system engineering or development lifecycle (SDLC) requirements. The goal of the Order Planning activity is to demonstrate understanding of the requirements by providing sufficiently detailed plans to ensure successful implementation and operation of the CDM capabilities. The contractor shall provide the following documentation under this sub-activity.

a. Proposed CMaaS System Implementation Architecture, showing sensors, dashboards, and connectivity.

b. Draft Security Accreditation package, describing the contractor's plan for implementing required security controls and its security model to prevent cross-propagation of malware across requesting organizations.

c. Proposed Concept of Operations, describing how the proposed architecture will meet the CMaaS requirements for the agency or community of agencies requesting services.

d. Plan for Transition to Production Operations from the existing architecture, including integrating existing tools and dashboards, if requested in the request for quote.

e. Plan for Production Operations, describing how the provider will operate the proposed architecture to meet CDM objectives.

f. Plan for Governance Support, describing how the provider will assist cooperating agencies to establish and coordinate governance of the CMaaS solution.

g. Requirements for any Government-Furnished Equipment/Government-Furnished Services on which the provider is relying to meet the CMaaS objectives.

h. Perform "as is" analysis on agency existing infrastructure to facilitate better CDM program and IT architecture planning.

Return To Top

TASK AREA 3 – SUPPORT CDM DASHBOARDS

The contractor shall provide the technical services necessary to install, configure, and maintain the envisioned DHS-provided Base CDM dashboard, any Intermediate (Summary or Object level) dashboards, or other agency-supplied dashboard or CDM reporting systems, for use by requesting organizations. The CDM dashboard function includes dashboards at different levels of the CDM architecture. These include "Top," "Intermediate," and "Base" dashboards, which may be further categorized as "Summary" or "Object-level" (as shown in Section 9 –Attachment O). The contractor shall all perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

Return To Top

TASK AREA 4 – PROVIDE-SPECIFIED TOOLS AND SENSORS

The contractor shall provide, install and configure a suite of CDM tools (as specified in an order) to perform / support the tool functional areas specified in Section 1: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, Vulnerability Management, Network and Physical Access Management, Trust Condition Management, Management of Security Related Behavior, Credentials and Authentication Management, Account Access Management, Contingency and Incident Preparation, Contingency and Incident Response, Design and Build in Requirements, Policy, and Planning, Design and Build in Quality, Operational Audit Information Management, Operational Security Management, and Management of other tools and sensors. If required by an order, these tools may include open source / public license software. In order to perform this task, orders may require the contractor to also provide, install, and configure ancillary IT hardware if needed to support the operation of the provided CDM tools. The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

Return To Top

TASK AREA 5 – CONFIGURE AND CUSTOMIZE TOOLS AND SENSORS

The contractor shall, according to the requirements of the requesting organization, customize the sensors and tools to accomplish the objective of assessing, for each capability, any deviations between the desired state of the IT asset and the actual state of the asset. This customization shall include the capability for the requesting agency to (1) record the desired state for authorized assets, (2) specify its own categories for grouping results, (3) customize scoring algorithms to quantify results, (4) customize grading standards for defect scores, and (5) establish responsibility for maintaining the desired state (and mitigating defects) of each assigned and discovered asset. Customization of software may include requirements to localize tools when required by an order. The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

Return To Top

TASK AREA 6 – MAINTAIN DATA ON DESIRED STATE FOR CDM TOOLS AND SENSORS

The contractor shall provide operational capability for the installed and configured tools and sensors that enables agencies to keep the data current for the desired state of target IT assets (baseline data), as needed, and on an ongoing basis.

Return To Top

CMAAS TASK AREA 7 – OPERATE CDM TOOLS AND SENSORS

The contractor shall operate the installed suite of CDM sensors to determine and report the actual state for functions within the periodicity specified in the order: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, Vulnerability Management, Network and Physical Access Management, Trust Condition Management, Management of Security Related Behavior, Credentials and Authentication Management, Account Access Management, Contingency and Incident Preparation, Contingency and Incident Response, Design and Build in Requirements, Policy, and Planning, Design and Build in Quality, Operational Audit Information Management, Operational Security Management, and Management of other tools and sensors. If defined in order requirements for supported agencies, the contractor shall also remove and remediate threats that are detected by the CDM tools and sensors. The contractor shall also perform all work necessary to maintain and provide end software

support to the tools and any ancillary hardware; including patching, upgrades, end-user support and replacement of failed components.

Return To Top

TASK AREA 8 – INTEGRATE AND MAINTAIN INTEROPERABILITY BETWEEN CDM TOOLS AND AGENCY LEGACY APPLICATIONS AND DATA

The contractor shall integrate CDM-operated tools and dashboard with associated agency information systems (as specified in the order) and maintain interoperability between the CDM tools and the agency data in operation. (For example, an agency might want to have data feeds exchanged between their existing property management system and the HWAM infrastructure.) The contractor shall also perform all appropriate quality assurance and technical testing to ensure the delivered tools perform to the requirements specified in the order.

Return To Top

TASK AREA 9 – OPERATE DATA FEEDS TO AND FROM INSTALLED DASHBOARDS

The contractor shall operate the DHS-provided dashboard to provide data feeds from the tools and sensors operated under Section 8 to the appropriate Intermediate dashboard(s) and any requested rollup (Summary or Object) dashboards (see Section 9 –Attachment O). The contractor shall operate data feeds between each operated dashboard and its parent dashboard. The contractor shall send data from the requesting organization's own summary dashboard (if installed and required by the order) to the DHS-provided dashboard. The contractor shall send data from the console of an existing sensor (if installed and required by the order) to the DHS provided dashboard. The contractor shall also provide the agency with a capability to retain all data within the agency-specified data retention criteria, if required by the requirements of an order. The contractor shall also perform all appropriate quality assurance and technical testing to ensure that data feeds perform to the requirements specified in the order.

Return To Top

TASK AREA 10 – TRAINING AND CONSULTING IN CDM GOVERNANCE FOR DEPARTMENTS, AGENCIES, AND OTHER REQUESTING ORGANIZATIONS

The contractor shall provide training and/or consulting to agencies and other requesting organizations to assist them in establishing an overall cybersecurity governance program with emphasis on using the continuous diagnostics to perform the most cost-effective mitigations within available resources. Training and consulting tasks are expected to include support for agency activities including, but not limited to:

a. Identification of and communication with stakeholders.

b. Assessing risk/priorities and agency readiness for transition.

c. Assist the Government with designing Federal scoring/grading to compare performance and progress of agencies to:

1. Ensure fairness and transparency in assessment, scoring, and grading.
2. Ensure validity and reliability in assessment, scoring, and grading.

d. Conducting No-Fault "Pilot" operation phase and transition from pilot to full operation.

e. Conducting Federal-level decision boards to:

1. Assign and transfer risk conditions.
2. Manage new or newly discovered risks.
3. Coordinate with US Computer Emergency Response Team (US-CERT), DHS' National Cyber Security Division (NCSD), etc.
4. Resolve configuration management issues.

5. Measure and manage sensor performance.
6. Resolve dashboard performance/usability issues (e.g., false positives, false negatives).
7. Coordinate standards and policies.

f. Providing agency manager assistance, such as:

1. Rollout Tiger Teams.
2. Help Desk support.
3. User group management.
4. Website to provide automated assistance/reference.

g. Assistance with Security Assessment and Authorization (formerly Certification and Accreditation) such as:

1. Models for using CDM results in ongoing Assessment and Authorization.
2. Models for using dashboards to meet plan of action and milestone (POA&M) requirements.

h. Coordination with agency office of inspector general (OIG) or Government Accounting Office (GAO) to support agency with audit compliance.

i. Establishing and maintaining an overall cybersecurity governance plan.

j. Other governance activities identified by DHS and/or agencies.

Return To Top

TASK AREA 11 – SUPPORT INDEPENDENT VERIFICATION & VALIDATION (IV&V) AND SYSTEM CERTIFICATION

The contractor shall provide the necessary engineering, project management, data, and documentation to support independent verification and validation (IV&V) efforts by third parties or Government personnel to accept / certify system or other deliverables as required by the order.

Return To Top