Continuous Diagnostics and Mitigation (CDM) Program

Tools and Continuous Monitoring as a Service (CMaaS)

Blanket Purchase Agreement (BPA)

Ordering Guide 2015

Please note that this document will be updated regularly. For the most recent version, please visit www.gsa.gov/cdm

Version 7.0 – September 2015

U.S. General Services Administration

TABLE OF CONTENTS

1.0 GENERAL INFORMATION

The General Services Administration (GSA), Federal Acquisition Service (FAS), Assisted Acquisition Services (AAS), Federal Systems Integration and Management Center (FEDSIM) offers all Federal Departments and Agencies (D/As), State, Local, Regional, and Tribal (SLRT) governments, and other authorized entities access to Continuous Monitoring products, services, and solutions though a Blanket Purchase Agreement (BPA). The Continuous Diagnostics and Mitigation (CDM) Program, Tools and Continuous Monitoring as-a-Service (CMaaS) BPA was established on behalf of the Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C), Continuous Diagnostics and Mitigation (CDM) Program.

2.0 BACKGROUND

In 2012, the Office of Management and Budget (OMB) identified continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority (CAP) goals, established in accordance with the Government Performance and Results Modernization Act.

To support federal D/As in meeting the CAP goal, DHS established the CDM Program, an implementation approach consistent with the Information System Continuous Monitoring (ISCM) methodology.

DHS, in partnership with the General Services Administration, established a government-wide acquisition vehicle for continuous monitoring capabilities. The CDM Tools/CMaaS BPA is available to federal, SLRT, and other authorized entities. The acquisition vehicle provides a consistent set of solutions at a reduced cost, which enhance the government's ability to identify and mitigate the impact of emerging cyber threats.

The CDM Tools/CMaaS BPA was awarded competitively against GSA IT Schedule 70 contracts in accordance with Federal Acquisition Regulation (FAR) 8.405-3, to 17 Industry teams, giving ordering activities access to over 130 CDM vendors and integrators via Contractor Teaming Arrangements (CTAs). It has a combined total estimated ceiling of $6 billion over the anticipated five-year period of performance.

3.0 PURPOSE OF ORDERING GUIDE

The purpose of this Ordering Guide is to provide a basic understanding of the processes that can be utilized to purchase products and/or services offered on the CDM Tools/CMaaS BPA.

4.0 APPLICABILITY

This Ordering Guide applies to all U.S. federal D/As, SLRT governments, and other GSA customers who plan to use the CDM Tools and CMaaS BPA[1].

In addition to this guide, DHS is serving as the ordering activity for consolidated federal CDM requirements. Federal D/As can contact DHS at CDM.FNR@HQ.DHS.GOV to determine qualification and availability. Detailed information on the consolidated federal CDM requirements and the DHS CDM Program, can be found on the Internet at www.dhs.gov/cdm.

[1] *GSA Order ADM 4800.2H, Eligibility to Use GSA Sources of Supply and Services, provides detailed information regarding the agencies and organizations that are eligible to use GSA sources.*

5.0 BENEFITS OF THE CDM TOOLS/CMAAS BPA

The CDM Tools/CMaaS BPA provides the opportunity to procure cyber tools and services that have undergone thorough technical capability reviews to ensure the products meet the functional areas of the CDM Program, and the standards required for government-wide implementation. Additionally, the BPA offers 34 tiered price bands, providing for cumulative quantity discounts for each product available for purchase.

6.0 ADMINISTRATION OF BPA

These CDM Tools/CMaaS BPA is administered by the GSA/FAS/AAS/FEDSIM CDM Program Office. Points of Contact are Angela Holden – angela.holden@gsa.gov, Contracting Officer (CO), and Randy Albert – randy.albert@gsa.gov, Program Manager and Contracting Officer's Representative (COR).

7.0 PERIOD OF PERFORMANCE

The Period of Performance (PoP) of the multiple award CDM Tools/CMaaS BPA is five years, consisting of a one-year base period and four, one-year options.

Base Period:	8/12/2013 – 8/11/2014
Option Period 1:	8/12/2014 – 8/11/2015
Option Period 2:	8/12/2015 – 8/11/2016
Option Period 3:	8/12/2016 – 8/11/2017
Option Period 4:	8/12/2017 – 8/11/2018

Orders awarded against the BPA will specify a PoP for the order. Order PoP shall not exceed the BPA PoP by more than one year.

This BPA, and orders issued thereunder, cannot be transferred to another GSA Schedule 70 contract. In the event a CTA Team Lead is removed or the Team Lead's GSA Schedule 70 contract has expired and additional option periods not exercised, a new Team Lead must be designated in order for that CTA's BPA to continue. In the event a prime contractor in a prime/sub arrangement loses its Schedule 70 contract, the BPA will not continue.

8.0 FUNDS OBLIGATION

The CDM Tools/CMaaS BPA award did not obligate any funds. Funds are obligated on orders issued by ordering activities.

9.0 BPA SCOPE

The CDM Tools/CMaaS BPA scope includes 15 Tool Functional Areas and 11 CMaaS Service Task Areas. Implementation will occur in three phases, listed below in Table 1. All Service Task Areas and Phase 1 Tool Functional Areas are available for ordering. Additional Tool Functional Areas mapped to Phases 2 and 3 will be implemented and made available for ordering as requirements develop. Phase 2 capabilities are estimated to be available for ordering in July of 2015.

Table 1.

Phase	Objectives	Tool Functional Area Implementation	Service Task Area Implementation
Phase 1	**Main Goal:** Endpoint Integrity **Scope:** Local Computing Environment (Devices) **Areas of Focus:** Hardware and Software Asset Management, Configuration Settings, Known Vulnerabilities, Malware	• Hardware Asset Management • Software Asset Management • Configuration Management *(Configuration Settings Management)* • Vulnerability Management	• Provide Order Project Management Support • CDM Order Planning • Support CDM Dashboards • Provide Specified Tools & Sensors • Configure & Customize Tools & Sensors • Maintain Data on Desired State for CDM Tools and Sensors • Operate CDM Tools & Sensors • Integrate & Maintain Interoperability between CDM Tools and Agency Legacy Applications and Data • Operate Data Feeds to and from Installed Dashboards • Training & Consulting in CDM Governance for D/As and other Requesting Organizations • Support Independent Verification & Validation (IV&V) & System Certification
Phase 2	**Main Goal:** Least Privilege & Infrastructure Integrity **Scope:** Local Computing Environment (People), Network & Infrastructure (Devices) **Areas of Focus:** Account & Privilege Management, Configuration Settings, and Ports/Protocols/Services for Infrastructure Devices	• Manage Trust in People Granted Access *(Access Control Management)* • Manage Security Related Behavior *(Security-Related Behavior Management)* • Manage Credentials and Authentication *(Credentials and Authentication Management)* • Manage Account Access *(Privileges)*	
Phase 3	**Main Goal:** Boundary Protection & Event Management **Scope:** Local Computing Environment (Events), Network & Infrastructure (Events), Enclave Boundary (Devices, Events) **Areas of Focus:** Audit & Event Detection/Response, Encryption, Remote Access, Access Control	• Prepare for Contingencies & Incidents *(Plan for Events)* • Respond to Contingencies & Incidents *(Respond to Events)* • Design and Build in Requirements, Policy and Planning *(Document Requirements, Policy, etc)* • Design and Build in Quality *(Quality Management)* • Manage Audit Information *(Generic Audit/Monitoring)* • Manage Operation Security *(Risk Management)* • Manage Network and Asset Controls *(Boundary Protection - Network, Physical, Virtual)*	**Estimated availability – 2016**

10.0 DESCRIPTION OF TOOL FUNCTIONAL AREAS

Tool Functional Area	Tool	Description
1	Hardware Asset Management	The Hardware Asset Management (HWAM) Function is to discover unauthorized or unmanaged hardware on a network. Once unauthorized or unmanaged hardware is discovered by the contractor's provided tool(s), the D/A will take action to remove this hardware. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.
2	Software Asset Management	The Software Asset Management (SWAM) Function is to discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Once unauthorized or unmanaged SWCI are discovered by the contractor's provided tool(s), the D/A will take action to remove these SWCI. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.
3	Configuration Management	The Configuration Management Function (CM) is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software. Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches. Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting federal agencies, and then pivot to attack other assets.
4	Vulnerability Management	The Vulnerability Management (VUL) Function is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. Once the contractor-provided tool(s) identify these mistakes and deficiencies, the D/A will take action to remove or remediate these from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network).
5	Manage Network Access Controls	The Manage Network Access Controls (NAC) Function is to prevent, and allow the agency to remove and limit unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest. Boundaries include firewalls as well as encryption (virtual private networks). Additionally, the function will prevent, remove, and limit unauthorized physical access.

Tool Functional Area	Tool	Description
6	Manage Trust-in-People Granted Access	The Manage Trust in People Granted Access (TRU) Function is to prevent insider attacks by carefully screening new and existing persons granted access for evidence that access might be abused. The Manage Trust in People Granted Access capability informs the Manage Account Access capability by providing background information and potential risk, or compromise, factors. These factors are used to determine if someone should be granted access, under the Manage Account Access capability, to certain resources (e.g., sensitive data).
7	Manage Security Related Behavior	The Manage Security Related Behavior (BEH) Function is to prevent general users from taking unnecessary risks to prevent attackers from exploiting network and application users via social engineering scams. BEH prevents users with elevated privileges and special security roles from taking unnecessary risks to prevent attackers from exploring poor engineering and/or remediation. The Manage Security Related Behavior capability addresses the behavior of someone who has been granted access to IT devices and systems. Information from this capability feeds into the Manage Trust in People Granted Access capability where determinations will be made about someone's suitability for continued access based, in part, on their behavior.
8	Manage Credentials and Authentication	The Manage Credentials and Authentication (MCA) Function is to prevent a) the binding of credentials to, or b) the use of credentials by other than the rightful owner (person or service) by careful management of credentials, preventing attackers from using hijacked credentials to gain unauthorized control of resources, especially administrative rights. The MCA capability ensures that account credentials are assigned to, and used by, authorized people. This capability will rely on the results of the Manage Account Access capability to ensure that only trusted people receive credentials. This covers credentials for physical and logistical access.
9	Manage Account Access	The Manage Account Access (MAA) Function is to prevent access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data. The MAA capability will assign access to computing resources based, in part, on their level of trustworthiness (as determined in Tool Functional Area 6).
10	Prepare for Contingencies and Incidents	The Prepare for Contingencies and Incidents (CP) Function is to prevent loss of confidentiality, integrity, and/or availability by being prepared for unanticipated events and/or attacks that might require recovery and/or special responses, preventing attacker's compromises from being effective by adequate recovery as needed, and natural events from causing permanent loss by adequate preparation as needed.
11	Respond to Contingencies and Incidents	The Respond to Contingencies and Incidents (INC) Function is to prevent repeat of previous attacks and limit the impact of ongoing attacks by using forensic analysis, audit information, etc. to a) appropriately respond to end ongoing attacks, and b) identify ways to prevent recurrence to prevent attackers from maintaining ongoing attacks and exploiting weaknesses already targeted by others.

Tool Functional Area	Tool	Description
12	Requirements, Policy, and Planning	The Design and Build in Requirements Policy and Planning (POL) Function is to prevent exploitation of the system by consciously designing the system to minimize weaknesses and building the system to meet that standard in order to reduce the attack surface and increase the effort required to reach the parts of the system that remain vulnerable. The POL capability includes software assurance best practices to ensure that security is built into the System Development Lifecycle. This capability addresses how to avoid or remove weaknesses and vulnerabilities before the system is released into production caused by poor design and insecure coding practices.
13	Design and Build-in Quality	The Design and Build in Quality (QAL) Function is to prevent attackers from exploiting weaknesses by finding and prioritizing weaknesses and fixing the most important weaknesses first. This capability addresses software before it is installed and operational.
14	Manage Audit Information	The Manage Audit Information (AUD) Function is to prevent persistent attacks and weaknesses by using audit information to identify them and initiate an appropriate response. The function addresses agency efforts to monitor the behavior of employees (for example, downloading pornography, unusual times/volumes of access, etc.). The results of these audits feed into the TRU capability where determinations will be made about someone's suitability for continued access based, in part, on their behavior.
15	Manage Operation Security	The Manage Operation Security (OPS) Function is to prevent attackers from exploiting weaknesses by using functional and operational control limits to help senior managers determine when to authorize operation of systems, and when to devote extra attention to reducing risks to prevent attackers from exploiting preventable weaknesses and analyze prior failures to identify and resolve system weaknesses. This activity receives information from the AUD capability to help support leadership decisions to enable improvement of security. It covers information about all operational capabilities and, therefore, does not apply to the creation of a system.
	Provide Ancillary Hardware	When required by orders under this BPA, the contractor shall provide ancillary IT hardware as needed to support the operation of the contractor's CDM Tool(s). All ancillary IT hardware must be on the contractor's GSA Schedule 70 contract or, in the event of a Contractor Teaming Arrangement (CTA), the contract of a teaming partner. The Government may allow the offeror to add a Contractor Teaming member after award if the Contracting Officer determines that it is in the best interest of the Government.

11.0 DESCRIPTION OF SERVICE TASK AREAS

Service Task Area	Service	Description
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 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
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

Service Task Area	Service	Description
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 of the BPA). 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.
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 2.2.1 of the BPA: 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.
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.
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.

Service Task Area	Service	Description
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.
8	**Integrate and Maintain Interoperability between CDM Tools and 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 its 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.
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 2.2.2.8 to the appropriate Intermediate dashboard(s) and any requested rollup (Summary or Object) dashboards (see Section 9 –Attachment O of the BPA). 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.
10	**Training and Consulting in CDM Governance for D/As 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 U.S. 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
11	**Support Independent Verification & Validation 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.

12.0 BPA AWARDEES (TEAM LEADS)

Awardee	BPA #
Booz Allen Hamilton	GS00T13AJA0008
CGI Federal, Inc.	GS00T13AJA0009
Computer Sciences Corporation	GS00T13AJA0010
Digital Management, Inc.	GS00T13AJA0011
Dynamics Research Corporation	GS00T13AJA0012
General Dynamics Information Technology	GS00T13AJA0013
Hewlett Packard Enterprise Services	GS00T13AJA0014
IBM Corporation	GS00T13AJA0015
Knowledge Consulting Group, Inc.	GS00T13AJA0016
Kratos Technology and Training Solutions, Inc.	GS00T13AJA0017
Leidos, Inc.	GS00T13AJA0022
Lockheed Martin Management Systems Designers, Inc.	GS00T13AJA0018
ManTech International Corporation	GS00T13AJA0019
MicroTech	GS00T13AJA0020
Northrop Grumman Systems Corporation	GS00T13AJA0021
SRA International, Inc.	GS00T13AJA0023
Technica Corporation	GS00T13AJA0024

13.0 CONTRACT TYPES

The CDM Tools/CMaaS BPA allows for the following order types:

- **Labor Hour (LH)** – The contract type used for level of effort projects with labor only.
- **Firm Fixed Price (FFP)** - This contract type should be used for nearly all commodity tool procurements, and any services procurement with a high level of definition in the performance work statement.
- **Cost Reimbursable (CR)** – Only travel portions of any GSA Schedule Order can be of a Cost-Reimbursable nature.

NOTE: Each Task Order/Delivery Order under the BPA can have a combination of contract types (e.g., LH for Labor, FFP for products, and CR for Travel)

The work shall be performed in accordance with this BPA and the awardees' GSA Schedule Contract (to include CTA Schedules, if applicable), under which the resulting BPA was placed. If a requirement includes a tool or labor category that is not on the awarded contractor's GSA Schedule (or the Contractor Teaming Partner's GSA Schedule), it cannot be purchased under the BPA.

14.0 FEES

14.1 Acquisition, Contracting, and Technical (ACT Fee)

The ACT fee is the cost of awarding, administering, and managing the CDM, Tools and CMaaS BPA. The ACT fee for this BPA is 2%, which shall be invoiced as a separate line item at the Task/Delivery Order level. This ACT fee is in addition to the Industrial Funding Fee (IFF). This fee applies only to tools and labor and does not apply to travel associated with the respective orders. Please note the ACT fee does not apply to orders issued by GSA or DHS.

The contractor shall electronically submit a Report of Sales to the BPA CO and COR, using the format in Section 9 – Attachment M of the BPA, within 15 days following the completion of the quarterly reporting period, or as requested by the BPA CO. Negative reports are required. The BPA CO and COR will provide written approval of each report. Once approved, the contractor shall submit the ACT fee. Remittance of the ACT fee shall be made by the contractor on a United States Government fiscal year (FY), quarterly basis (e.g., October-December, January-March, April-June, July-September) or as otherwise requested by the BPA Contracting Officer (BPA CO).

ACT fees that have not been paid within 30 calendar days of report approval by the BPA CO shall be considered a debt to the United States Government under the terms of FAR 32.6 Contract Debts. The Government may exercise all its rights under the BPA, including withholding or setting off payments and interest on the debt (see FAR clause 52.232-17, Interest). Failure of the contractor to pay the ACT fee in a timely manner may result in termination of the BPA.

14.2 FEDSIM Fees

For those acquisitions in which the requesting agency elects to have GSA/FAS/AAS/FEDSIM provide full or partial acquisition and/or project management support services to assist in making an award on the BPAs, a FEDSIM fee is negotiated on an order-by-order basis between FEDSIM and the requesting agency. See the AAS ordering option in Section 16 of this ordering guide for more details.

15.0 SECURITY

The CDM Tools/CMaaS BPA awardees are responsible for provisioning, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present the CDM Program solutions to the consumer.

Prior to accepting an order from an ordering activity, the CDM Tools/CMaaS BPA awardees are responsible for reviewing and complying with the applicable security requirements in the BPA.

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A) with continuous monitoring. The NIST Special Publication (SP) 800-37, Revision 1, "Guide for applying the Risk Management Framework to Federal Information System" (hereafter described as NIST 800-37), gives guidelines for performing the A&A process. In addition, NIST SP 800-53 provides guidance regarding appropriate controls for each system.

An independent third-party assessment may be required by orders under this BPA of the contractor's security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The ordering activity's security assessment staff will be available for consultation during the process, and will review the results before issuing an Assessment and subsequent Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

The contractor is advised to review the NIST documents to determine the level of effort that will be necessary to complete the requirements.

Ordering activities, including non-federal entities such as state governments, may have other security provisions defined at the order level.

16.0 ORDERING OPTIONS

The following options are available for ordering products and services off of the CDM Tools/CMaaS BPA:

1. Coordinate with DHS as the ordering activity for consolidated federal CDM requirements
2. Direct Order/Direct Bill (DO/DB) via Delegated Procurement Authority (DPA)
3. Assisted acquisition/consulting services (AAS)

16.1 DHS Process

Federal D/As can also participate in the CDM Program through a Memorandum of Agreement (MOA) the DHS Program Office. Interested organizations should contact cdm.fnr@hq.dhs.gov for more information regarding participation in the CDM Program and eligibility requirements.

Before placing a DO/DB requirement against the BPA, it is recommended that agencies communicate with their CIO offices to avoid duplicative agency procurement efforts that might be ongoing via MOA with the CDM Program.

16.2 Direct Order / Direct Bill

Federal D/As, SLRT governments, and other entities authorized to utilize GSA Federal Supply Schedules may order products and services off the CDM Tools/CMaaS BPA by requesting a DPA from the GSA/FAS/AAS/FEDSIM CDM Tools/CMaaS BPA Contracting Officer. A DPA must be granted prior to any DO/DB orders being placed.

Once authority is granted, customers will interact directly with the CMaaS BPA awardees to place orders. With DO/DB orders, the agency is responsible for all aspects of the acquisition and administration of Task Orders. The agency Contracting Officer or designee will be subject to the FAR, rules, regulations, and conditions promulgated and enforced by that agency. Billing for products and services is directly between the ordering agency and the CDM Tools/CMaaS BPA order awardees.

16.3 Assisted Acquisition Services

Organizations may elect to have GSA/FAS/AAS/FEDSIM provide acquisition and/or project management services to assist in procuring CMD Tools/CMaaS products and services. If the requesting agency utilizes this option, FEDSIM will support the issue of, modification, administration, and closing of orders based on the requesting agency's requirements for support as documented in an Interagency Agreement (IA) signed by both parties (i.e., Reference OMB memo dated June 6, 2008, Improving the Management and use of Interagency Acquisitions).

AAS works through IAs to establish the service-level expectation, schedule, and funding mechanism. As a cost-reimbursable, non-appropriated organization, services are offered on a fee-for-service basis and include hourly rates, fixed-price, and surcharge options.

17.0 DIRECT ORDER / DIRECT BILL PROCESS

17.1 Delegation of Procurement Authority (DPA)

The first step in the DO/DB process is completing the DPA. This must be accomplished prior to any DO/DB orders being placed and consists of a signed letter from the GSA/FAS/AAS/FEDSIM CDM Tools/CMaaS BPA Contracting Officer to an authorized procurement agent at the requesting agency. DPAs provide rules and procedures for utilizing the contract vehicle, and also authorize access to the BPA, and pricing.

To establish a DPA, an requesting agency's Ordering Contracting Officer (OCO)/Authorized agent sends an email to cdm@gsa.gov, providing a copy of their warrant and the dollar threshold to which they are authorized to purchase. Once received, GSA FEDSIM will review and process and provide the OCO with a DPA letter. This letter outlines the roles and responsibilities the OCO has for utilizing this vehicle over the entire period of performance of the BPA. In addition, once the DPA is granted - the OCO will receive access to the detailed pricing for the products and services under this BPA.

17.2 Scope Determination

After a DPA has been established, it is important to determine if the requirement is within scope of the CDM Tools/CMaaS BPA, as defined by CDM Tools/CMaaS BPA Request for Quote (RFQ), including Attachment N (Tool Requirements).

If further assistance is needed to determine whether the requirements is within scope, please contact GSA FEDSIM CDM CO and COR at CDM@gsa.gov.

17.3 Statement of Work (SOW) / Performance Work Statement (PWS)

Once the OCO has determined that the requirement is within scope to the CDM Tools/CMaaS BPA, a SOW must be prepared by the requiring agency.

The SOW/PWS typically includes:

- Scope of Work to be Performed
- Performance Objectives
- Requirements
- Period of Performance
- Deliverables

The location of work (or place of performance or delivery) will be included in each individual order issued under this BPA, and defines where the service or commodity tool is required. Long-distance and overseas travel may be required to perform work under an individual order and will be detailed within the order, if required.

17.4 Request for Quote (RFQ)

The requesting agency will follow its usual procedures for preparing an RFQ, including following any internal policy and procedures related to acquiring IT products and services.

Each individual RFQ may be LH, FFP, or any combination of the two. For any order that is other than FFP, the ordering activity shall include, at a minimum, the documentation outlined in FAR 8.405-2(e). The RFQ may include specific metrics and quality assurance methods (if applicable).

All RFQs will incorporate all terms and conditions of the BPA. In addition, the proposed RFQ will include the following to the extent applicable to individual orders:

a. An SOW or other performance-based work statement describing the work to be performed, the deliverables, the period of performance, Government Points of Contact (POCs), description of marking information, data rights, inspection and acceptance of services, security requirements, and Government-Furnished Information / Property, as applicable.
b. The submission date/time and the method of delivery for quotes.
c. Specific instructions on what to include in the quote submission. This may include, but is not limited to, written responses summarizing technical and price approaches.
d. Evaluation factors.
e. Other information deemed appropriate.

17.5 Task Order Value and Funding Type

Estimate the value of the order. For orders that are expected to exceed $1,000,000, the OCO must include language in the RFQ which indicates the intent to seek additional discounts. A multi-year order placed under the BPA must be consistent with FAR Subpart 17.1 and any applicable funding restrictions.

17.6 Issuing the RFQ

The OCO may issue orders under the BPA pursuant to the procedures in FAR subpart 8.4; more specifically, all ordering procedures required by FAR 8.405-3(c)(2) apply to orders issued under the BPA. OCOs are required to solicit requirements to all 17 BPA awardees, unless an exception applies per FAR subpart 8.4, and a determination is made by the OCO. Zero or more orders may be issued during the performance period of this BPA; it is understood and agreed that the Government has no obligation to issue orders. The contractor agrees to accept and perform orders issued by a CO from any department or agency of the Federal Government within the scope of this agreement. Contractor acceptance of orders from SLRT governments is voluntary. In the event of a conflict between an order, the BPA, or the contractor's GSA Schedule contract, the GSA Schedule contract takes precedence.

In accordance with the issued DPA, the OCO is required to notify the BPA Contracting Officer and COR prior to issuing an RFQ on the BPA, and prior to making an award. This is to ensure sufficient ceiling is available on the BPA, and to communicate any updates to price bands that might be available.

To issue the RFQ, OCOs are encouraged to utilize GSA eBuy (www.ebuy.gsa.gov) to solicit the BPA awardees. The CDM Tools/CMaaS BPA is available as a vehicle to be chosen on eBuy, and quotes or sources sought postings will be automatically distributed to the 17 BPA awardees through this method.

If the OCO or ordering office would prefer to utilize email as a method of soliciting, please contact the BPA CO and COR for up to date email contact information for each of the BPA awardees.

17.7 Evaluate

After the RFQ closes, the ordering activity evaluates all responses received using a selected evaluation approach. For example, an ordering activity could select the BPA awardee that represents the best value. Ordering activities determine their own evaluation criteria. See FAR 8.4052 (d) for additional guidance on this topic.

17.8 Price Reductions

Notwithstanding the BPA pricing discounts, ordering activities are encouraged and empowered to seek further price reductions when issuing orders under the CMaaS BPA.

17.9 Award

The ordering activity shall place the order as it would for any other fixed-price Multiple Award Schedule TO in accordance with FAR 8.406-1.

In accordance with the BPA and FAR 8.405-2(e), ordering activities shall document the following:

- Note the BPA holder receiving the TO and all BPA awardees that were considered.
- Description of what was purchased and agreed upon pricing.
- The evaluation methodology used in selecting the BPA holder to receive the TO.
- The rationale for any tradeoffs in making the selection.
- The price reasonableness determination required by FAR 8.405-2(d).
- The rationale for using other than a performance-based order.

Helpful hints to consider when preparing and awarding the TO: *Make sure that the BPA number, the BPA holder's name and Schedule Contract Number are included on all orders. Refer to FAR 8.406-1 for information to be included on orders.*

17.10 Order Administration

Upon award, OCOs are responsible for entering Order information into the Federal Procurement Data System – Next Generation (FPDS-NG),if/ as applicable. In addition to FPDS-NG reporting, OCOs are required to provide a complete copy of the Order, e.g., (equivalent to Sections A-J of the Uniform Contract Format as prescribed by the Federal Acquisition Regulation) and the signature page. OCO's are also required to provide any subsequent modifications that impact the value of the initial award. The OCO's shall provide the Order award and any subsequent modifications utilizing the Order Information Form(s) included with their DPA. The Order Information Form shall be submitted to the respective CDM email address within five days of award.

18.0 MORE INFORMATION

For more information regarding the CDM Program and the CDM Tools/CMaaS BPA, visit:

General Services Administration	www.gsa.gov/cdm
Department of Homeland Security	www.dhs.gov/cdm
U.S. Computer Emergency Readiness Team	https://www.us-cert.gov

All inquiries regarding the GSA FEDSIM CDM/CMaaS BPA, should be directed to the following:

CDM Tools/CMaaS BPA	
Program Office	CDM@gsa.gov

ATTACHMENT 1.0 CHANGE LOG

Version	Date	Description
1.0	Aug 2013	Initial Approval
2.0	Sep 2013	Revision
3.0	Oct 2013	Revision
4.0	Mar 2014	Revision
5.0	May 2015	Revision
6.0	Jul 2015	Revision
7.0	Sep 2015	Revision