Continuous Diagnostics and Mitigation (CDM) Program

Tools and Continuous Monitoring as a Service (CMaaS)

Blanket Purchase Agreements

Ordering Guide 2013

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

Version 3.0 – October 2013

GSA/FAS/AAS/FEDSIM

The General Services Administration (GSA), Federal Acquisition Service (FAS), Assisted Acquisition Services (AAS), Federal Systems Integration and Management Center (FEDSIM) offers Department of Homeland Security (DHS) and all Federal Departments and Agencies (D/As), state, local, regional, and tribal governments access to multiple Blanket Purchase Agreements (BPAs) that offer Continuous Monitoring as a Service (CMaaS)-related products, services, and solutions with cumulative stair-step pricing discounts. These BPAs were established on behalf of the DHS, Office of Cybersecurity and Communications (CS&C), Continuous Diagnostics and Mitigation (CDM) Program.

PURPOSE OF ORDERING GUIDE:

The purpose of this Ordering Guide is to provide an understanding of the products and services being offered through the BPAs, the companies who have been awarded BPAs, and the ordering options available to purchase products and/or services offered on the CDM Tools/CMaaS BPAs.

This Ordering Guide provides four BPA ordering options which will be explained in more detail in the following pages of this guide. These options include:

1. Federal Agencies' use of the Direct Order/Direct Bill option to procure products and or/services from the CDM Tools/CMaaS BPAs via Delegated Procurement Authority (DPA).
2. State, local, regional and tribal governments' use of the Direct Order/Direct Bill option to procure products and or/services from the CDM Tools/CMaaS BPAs via DPA.
3. Federal Agencies' use of assisted acquisition/consulting services from GSA AAS FEDSIM or a GSA FAS Regional AAS Customer Service Center to acquire full life-cycle acquisition support for their procurement of CDM Tools/CMaaS products and/or services.
4. Federal Agencies' use of the DHS process to procure products and/or services from the CDM Tools/CMaaS BPAs via Memorandum of Agreement between DHS and the Agency.

In developing these BPAs, GSA AAS FEDSIM simplified ordering by providing:

- Access to high-quality industry partners.
- Pre-competed, multiple-award BPAs.
- Shorter procurement lead time.
- Socio-economic credit through Federal Procurement Data System – Next Generation (FPDS-NG) reporting.
- Consistent service categories for all vendors.
- Customer-focused staff with experience in technology acquisitions.
- Available scope compatibility reviews of prospective orders and modifications.
- Acquisition support.

HOW TO REACH US:

Customers should contact the GSA FEDSIM CDM Program Office at CDM@gsa.gov or by contacting one of the following Points of Contact:

CDM Tools/CMaaS BPA Contracting Officer's Representative
Cristen Cole
Cristen.Cole@gsa.gov

CDM Tools/CMaaS BPA Contracting Officer
Anissa Burley
Anissa.Burley@gsa.gov

MORE INFORMATION:

Customers can find more information regarding the CDM Program and the CDM Tools/CMaaS BPAs at the following sites:

www.gsa.gov/cdm

www.dhs.gov/cdm

Table of Contents

Table of Contents

1.0 GENERAL INFORMATION

1.1 BACKGROUND

The Department of Homeland Security (DHS) has a mission to safeguard and secure cyberspace in an environment where the cyber attack threat is continuously growing and evolving. The Continuous Diagnostics and Mitigation (CDM) program seeks to defend Federal Information Technology (IT) networks from cyber-security threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, dashboards, and Continuous Monitoring as a Service (CMaaS) to strengthen the security posture of Government networks.

The CDM Tools/CMaaS Blanket Purchase Agreements (BPAs) were awarded competitively against GSA IT Schedule 70 contracts in accordance with Federal Acquisition Regulation (FAR) 8.405-3. They have a combined total estimated ceiling of $6 billion over the anticipated five-year period of performance.

1.2 APPLICABILITY

The Ordering Guide applies to DHS and all U.S. Federal Departments and Agencies (D/As), state, local, regional, and tribal governments, and other GSA customers who plan to use the CDM Tools and CMaaS BPAs. All customers may award orders against these BPAs.

These BPAs may be used by any entity within the executive branch of government, and by state, local, and tribal governments and other entities as listed in GSA Order ADM 4800.2G, Eligibility to Use GSA Sources of Supply and Services, which provides detailed information regarding the agencies and organizations that are eligible to use GSA sources.

1.2.1 DHS Support of the CDM Tools/CMaaS BPAs:

DHS has been given the authority and funding for the CDM program to strengthen the cybersecurity posture of the Federal civilian ".gov" networks. By centrally managing and funding this program, and in consultation with other stakeholders such as the Office of Management and Budget (OMB), the National Security Staff (NSS), and the National Institute of Standards and Technology (NIST), DHS will be able to work with D/As to evolve a consistent approach to continuous monitoring on the part of the Federal Government, making available an approach that meets minimum critical requirements, and leverages centralized acquisition to improve the speed of procurement and achieve significant discounts by consolidating like Federal requirements into "buying groups." This initiative is also in direct support of the Administration's 2014 Cross-agency Priority (CAP) goal for implementing continuous monitoring across the Federal networks.

DHS will have a CDM order mechanism available for qualifying Federal Agencies, which will require Federal Agencies to contact DHS in order to determine qualification and availability. Detailed information on this mechanism and the DHS CDM Program can be found on the Internet at www.dhs.gov/cdm. Queries can be sent via email to CDM.FNR@HQ.DHS.GOV.

1.3 BPA SCOPE

Section 1 (SUPPLIES/SERVICES AND PRICES/COST) and Section 2 (STATEMENT OF WORK) of the CDM Program, Tools and CMaaS BPA (GSC-QF0B-13-32662) are available upon written request to the BPA COR, CO, or the GSA FEDSIM CDM Program Office – cdm@gsa.gov.

GSA/FAS/AAS/FEDSIM established multiple award BPAs to provide DHS and all U.S. Federal D/As, state, local, regional, and tribal governments with specialized IT services and tools to implement DHS' CDM Program. The CDM program seeks to defend Federal IT networks from cyber security threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, dashboards, and CMaaS to strength the security posture of Government networks.

The scope of the CDM, Tools/CMaaS BPAs includes 15 Tool Functional Areas and 11 CMaaS Service Task Areas. At the time of BPA award, only the first four Tool Functional Areas will be available for ordering, along with the 11 CMaaS Service Task Areas. As future requirements develop, the additional Tool Functional Areas will be made available for ordering.

Tool Functional Areas	Service Task Areas
1- Hardware Asset Management	1- Provide Order Project Management Support
2- Software Asset Management	2- CDM Order Planning
3- Configuration Management	3- Support CDM Dashboards
4- Vulnerability Management	4- Provide Specified Tools and Sensors
*5- Manage Network and Asset Controls**	5- Configure and Customize Tools and Sensors
*6- Manage Trust and People Granted Access**	6- Maintain Data on Desired State for CDM Tools and Sensors
*7- Manage Security Related Behavior**	7- Operate CDM Tools and Sensors
*8- Manage Credential and Authentication**	8- Integrate and Maintain Interoperability between CDM Tools and Agency Legacy Applications and Data
*9- Manage Account Access**	
*10- Prepare for Contingencies and Incidents**	9- Operate Data Feeds to and from Installed Dashboards
*11- Respond to Contingencies and Incidents**	
*12- Design and Build in Requirements Policy and Planning**	10- Training and Consulting in CDM Governance for Departments, Agencies, and other Requesting Organizations
*13- Design and Build in Quality**	
*14- Manage Audit Information**	11- Support Independent Verification and Validation (IV&V) and System Certification
*15- Manage Operation Security**	

*Not available at time of award

1.3.1 DESCRIPTION OF TOOL FUNCTIONAL AREAS:

TOOL FUNCTIONAL AREA 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 agency 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.

TOOL FUNCTIONAL AREA 2 - SOFTWARE ASSET MANGEMENT

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 agency 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.

TOOL FUNCTIONAL AREA 3 – CONFIGURATION MANAGEMENT

The Configuration Management (CM) Function is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software. Once a misconfiguration of hardware devices is discovered by the contractor provided tools, the supported DAs will be responsible to take any needed action to resolve the problem or accept the risk. 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.

TOOL FUNCTIONAL AREA 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 agency 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.).
Not available for ordering at this time:

TOOL FUNCTIONAL AREA 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 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).

TOOL FUNCTIONAL AREAS 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.

TOOL FUNCTIONAL AREA 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.

TOOL FUNCTIONAL AREA 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).

TOOL FUNCTIONAL AREA 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.

TOOL FUNCTIONAL AREA 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 12 – DESIGN AND BUILD IN 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.

TOOL FUNCTIONAL AREA 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.

TOOL FUNCTIONAL AREA 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.

TOOL FUNCTIONAL AREA 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.

1.3.2 DESCRIPTION OF SERVICE TASK AREAS:

CMAAS 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.

CMAAS 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.

CMAAS 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 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.

CMAAS 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 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.

CMAAS 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.

CMAAS 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.

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.

CMAAS 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 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.

CMAAS 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 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.

CMAAS 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 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.

CMAAS 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.

1.4 BPA AWARDEES (CTA 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
Lockheed Martin Management Systems Designers, Inc.	GS00T13AJA0018
ManTech International Corporation	GS00T13AJA0019
MicroTech	GS00T13AJA0020
Northrop Grumman Systems Corporation	GS00T13AJA0021
SAIC	GS00T13AJA0022
SRA International, Inc.	GS00T13AJA0023
Technica Corporation	GS00T13AJA0024

1.4.1 BPA AWARDEE POINTS OF CONTACT (POCs)

See Attachment 1 – BPA Awardee Points of Contact.

1.5 CONTRACT TYPE

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)** - It is recommended this contract type should be used for nearly all commodity 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.

Each TO/DO can have multiple contract types (e.g., LH for CLIN 0005, FFP for CLIN 0001, and CR for Travel for CLIN 0007).

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. This means that if a requirement includes something 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.

1.6 FEES

1.6.1 ACT FEE

The cost of awarding, administering, and managing this BPA is included in the prices delineated in Section 1 – Supplies or Services and Price/Costs of the BPA. The Acquisition, Contracting, and Technical (ACT) fee for this CDM Tools CMaaS BPA is 2%, which will be invoiced as a separate line item. This ACT fee is in addition to the Industrial Funding Fee (IFF); there is no cap on the fee and can be applied incrementally with incremental funding modifications. Contractors shall include this fee for Tool device licenses and CMaaS labor rate price quotes and should note that it does not apply to travel costs. Please note the ACT fee does not apply to orders issued by GSA.

Remittance of the ACT fee shall be made by the contractor on a U.S. 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). The contractor shall electronically submit a Report of Sales to the BPA CO, 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 will provide written approval of each report, as well as a request to remit ACT fees.

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 U.S. 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.

1.6.2 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 services through the BPA's life cycles, a FEDSIM fee is negotiated on an order-by-order basis between FEDSIM and the requesting agency.

1.7 FUNDS OBLIGATION

The CDM Tools/CMaaS BPAs awards did not obligate any funds. Funds will be obligated on orders issued by ordering activities.

1.8 PERIOD OF PERFORMANCE

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

Base Period: 08/12/2013 – 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 the BPA to continue. In the event a prime contractor in a prime/sub arrangement loses its Schedule 70 contract, the BPA will not continue.

1.9 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 which are available in the BPA.

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization 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 Assessment and Authorization (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. For purposes of background information, typical security clauses for DHS orders are provided at Section 9 - Attachment J of the BPA.

1.10 ADMINISTRATION OF BPAs

These CDM Tools/CMaaS BPAs will be administered by the GSA / FAS / AAS / FEDSIM CDM Program Office. Points of Contact are Cristen Cole, Contracting Officer's Representative (COR), Cristen.Cole@gsa.gov and Anissa Burley, Contracting Officer (CO), Anissa.Burley@gsa.gov.

2.0 ORDERING OPTIONS

As mentioned above, there are several options available for ordering products and/or services off of the CDM Tools/CMaaS BPAs. This section will provide details regarding each of the options.

2.1 Federal Agencies' use of the Direct Order/Direct Bill option to procure products and or/services from the CDM Tools/CMaaS BPAs via Delegated Procurement Authority (DPA).
2.2 State, local, regional and tribal governments use of the Direct Order/Direct Bill option to procure products and or/services from the CDM Tools/CMaaS BPAs via DPA.
2.3 Federal Agencies' use of assisted acquisition/consulting services from GSA AAS FEDSIM or a GSA FAS Regional AAS Customer Service Center to acquire full life-cycle acquisition support for their procurement of CDM Tools/CMaaS products and/or services.
2.4 Federal Agencies' use of the DHS process to procure products and/or services from the CDM Tools/CMaaS BPAs via Memorandum of Agreement between DHS and the Agency.

Note: It is the responsibility of the ordering activity Contracting Officer to ensure compliance with all applicable fiscal laws and acquisition regulations prior to issuing an order under a CDM Tools/CMaaS BPA, and to ensure that the BPA holder selected provides the best value for the requirement being ordered.

CLASSIFIED ORDERS:

Unclassified deliverables or correspondence shall be delivered to the order CO or COR at the address specified in the order.

This BPA is set up to handle classified requirements. Any classified requirement will have to be handled in accordance with all appropriate security guidelines, FAR, and agency-specific regulations.

2.1 DIRECT ORDER/DIRECT BILL

Delegation of Authority (DPA): A DPA must be requested from the GSA/FAS/AAS/FEDSIM Contracting Officer (identified in Section 1.10) and granted prior to any Direct Order/Direct Bill (DO/DB) orders being placed. Once authority is granted, customers may interact directly with the CMaaS BPAs' contractors for communication and to place orders. With DO/DB, orders the agency is responsible for all aspects of the acquisition and administration of Task Orders (TOs)/DOs. The client agency Contracting Officer or designee will be subject to the FAR, rules, regulations, and conditions promulgated and enforced by that agency. The billing for these services is directly between the Ordering Agency and the CDM Tools/CMaaS BPAs' contractors.

The client agency is responsible for its own acquisition and program management activities. After the client agency Contracting Officer has received a DPA to become the Ordering Contracting Officer (OCO), the OCO is authorized to issue, modify, administer, and close orders.

2.2 STATE, LOCAL, REGIONAL, AND TRIBAL USE OF THE BPAS

State, local, regional, and tribal governments must follow their own acquisition regulations to meet competition thresholds and requirements when buying through GSA Schedules and this CDM

Tools/CMaaS BPA. To incorporate GSA terms and conditions, list the CDM Tools/CMaaS BPA Number on the TO/DO.

State, local, regional, and tribal governments are encouraged, but not required, to use GSA's Schedule Ordering Procedures to ensure competition and to receive the best value from GSA Schedule contractors. Ordering Procedures for use of GSA Schedules can be found at the following two sites: http://www.gsa.gov/portal/category/100631 and http://www.gsa.gov/portal/category/100639.

Ordering Procedures for Supplies and Services Not Requiring a Statement of Work (FAR 8.405-1) or the Ordering Procedures for Services Requiring a Statement of Work (FAR 8.405-2) are examples of best practice.

2.3 ASSISTED ACQUISITION SUPPORT

AAS works through Interagency Agreements (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.

A requesting agency may elect to have GSA/FAS/AAS/FEDSIM provide full or partial acquisition and/or project management services through the BPAs life cycles. If the requesting agency uses GSA/FAS/AAS/FEDSIM, GSA/FAS/AAS/FEDSIM will act as the OCO and will issue, modify, administer, and close orders based on the requesting agency's requirements for support. These responsibilities are documented in an IA signed by both parties (i.e., Reference OMB memo dated June 6, 2008, Improving the Management and use of Interagency Acquisitions).

CONSULTING AND ORDERING SERVICES THROUGH GSA/FAS/AAS/FEDSIM:

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.

A requesting agency may elect to have GSA/FAS/AAS/FEDSIM provide partial acquisition and/or project management services through the BPAs TO/DO life cycles. If the requesting agency uses GSA/FAS/AAS/FEDSIM, GSA/FAS/AAS/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 IA signed by both parties (i.e., Reference OMB memo dated June 6, 2008, Improving the Management and use of Interagency Acquisitions).

2.4 USE OF DHS PROCESS

Each Federal Agency participating must sign a Memorandum of Agreement (MoA) with DHS, and participate in surveys, questionnaires, meetings and conference calls to confirm requirements.

Based on the information in Agency-provided foundational surveys and after consultation with Agencies, DHS intends to execute TOs against the BPA for specific groups of agencies that require common solutions.

By grouping Agencies into like-requirements, DHS is able to leverage stair-step, volume discount pricing and achieve efficiencies in developing, processing, and managing TOs.

Contact cdm.fnr@hq.dhs.gov or visit www.dhs.gov/cdm for further information.

3.0 PLACING AN ORDER AGAINST THE CDM TOOLS/CMAAS BPA

This section provides the acquisition process for placing an order under the CDM Tools/CMaaS BPAs.

3.1 SCOPE DETERMINATION

When establishing ordering activity requirements, it is important to first determine if the requirement is within scope of the CDM Tools/CMaaS BPAs, 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 are within scope, please contact GSA FEDSIM CDM Program Office at CDM@gsa.gov.

3.2 PREPARE STATEMENT OF WORK (SOW) OR PERFORMANCE WORK STATEMENT (PWS)

The Statement of Work (SOW)/Performance Work Statement (PWS) typically includes:

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

Please contact the GSA FEDSIM CDM Program Office for a sample SOW/PWS template, if needed, at CDM@gsa.gov.

3.2.1 LOCATION OF WORK

The location of work (or place of performance or delivery) will be defined in the individual order issued under this BPA. It is where the service or product 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.

3.3 PREPARE THE REQUEST FOR QUOTE (RFQ)

Follow your agency's 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.

3.3.1 TASK ORDER VALUE & FUNDING TYPE

Estimate the value of the order. For orders that are expected to exceed $1,000,000 you must include language in the RFQ which indicates your 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.

3.4 ISSUE THE RFQ

Prior to issuing an order solicitation, and making an order award, the OCO must contact the BPA CO (see Section 1.10 above) to request ordering authority. This will ensure the order value is within the total BPA value, ensure volume discounts are being properly applied, and answer any questions of scope or modification. Only those that have received ordering authority may place Orders under the BPA.

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. 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 state, local, regional, and tribal 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.

3.5 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.

3.5.1 PRICE REDUCTIONS

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

3.6 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.

3.6.1 DOCUMENTATION

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 holders 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.

The below are some 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.

3.7 ORDER ADMINISTRATION

Contracting Officers (COs) and Contracting Officer Representatives (CORs) may be appointed at a TO level by the ordering activity.

The below table outlines the predefined management reporting requirements for the CMaaS BPAs as defined in the BPA. There are requirements for the awardees for both providing these reports accessible via online interface not later than 10 days after the end of the calendar month, as well as hard copy/electronic copy requirements for delivering to the ordering activity COR.

The predefined reporting requirements for the CMaaS/Tools BPAs are shown below:

Report(s)	Due Date	Report Initiator	Recipient(s)
Written notification of new, Fully Executed Order (includes – Order Name and Number; Name of Funding Agency POC; Name of Award Agency POC; Period of Performance; Estimated Dollar Value). Complete Copy of Order.	Within 10 days of Task Order award	BPA Holder	BPA Contracting Officer BPA Project Manager

Report(s)	Due Date	Report Initiator	Recipient(s)
Quarterly Report of Sales for CMaaS Services, and Products	NLT Day 15 after the end of each quarter (April, June, September, and December)	BPA Holder	BPA Contracting Officer BPA Project Manager
Orders utilizing Recovery Funds	NLT Day 10 after the end of each quarter (April, June, September, and December)	BPA Holder	www.FederalReporting.gov

ATTACHMENT 1 - BPA AWARDEE POINTS OF CONTACT				
VENDOR	**NAME**	**CONTACT INFO**	**EMAIL**	**PHONE**
Booz Allen Hamilton	Judith-Ann Martin	Contracts Manager	martin_judithanne@bah.com	703.377.0012
	William Hilsman	Program Manager	hilsman_william@bah.com	703.902.4887
	CMaaS BPA Ordering		cmaas@bah.com	
CGI Federal, Inc.	John Heneghan	CMaaS Program Manager	john.p.heneghan@cgifederal.com	703.227.7562
	Steven Frazier	Contract Administrator	steve.frazier@cgifederal.com	703.227.4702
	CMaaS Inquiries		cmaas@cgifederal.com	
Computer Sciences Corporation	Fernando Pidal	Manager, Contracts & Commercial Management	fpidal@csc.com	202.874.7736
	Josh F Canary	CMaaS BPA PM	jcanary@csc.com	703..908.7030
Digital Management, Inc.	Rick Roach	CDM CMaaS Program Manager	rroach@dminc.com	240.223.4800
	Jason Klewe	CDM CMaaS Project Manager	jklewe@DMInc.com	703.297.8490
	Thelma Miles	Senior Contracts Manager	tmiles@DMInc.com	240.720.0404
	Carmen Bayran	Contracts Manager	cbayran@DMInc.com	240.720.0433
Dynamics Research Corporation	Bryan Hennessy		bhennessy@drc.com	401.872.5368
	Eric Wolf	VP & General Manager, Homeland Security Division	ewolf@drc.com	571.226.8629
GDIT	Lee Canterbury	Program Manager	lee.canterbury@gdit.com	703.966.5868
	Pamela Azar	Contracts	pamela.azar@gdit.com	703.858.2477
	Steven Felber	Contracts Alternate	gditgsa@gdit.com	703.885.1906
HPES	Dorothy Pines	Contract Manager	dorothy.pines@hp.com	703.742.2158
	Gregg Hawrylko	BPA Program Manager	hawrylko@hp.com	703.733.3008
IBM	Christopher Ballister	IBM Associate Partner	cmballis@us.ibm.com	410.353.1733
	John W. Lainhart IV	IBM Partner	john.w.lainhart@us.ibm.com	301.803.2745
	CDM Inquiries		dhscdm@us.ibm.com	
KCG	Matt Brown	Vice President and CDM Program Director	matt.brown@knowledgecg.com	202.256.7500
	Ryan McCullough	GovPlace, VP Federal Division	rmccullough@govplace.com	240.381.2937
	Beth Beach	TASC, Director Cybersecurity	beth.beach@tasc.com	703.677.6093
Kratos	Patrick Howard	Program Manager	cdm@secureinfo.com	210.403.5600
Lockheed Martin	Robert L. Morgan III	Sr. Staff Contracts Negotiator	robert.l.morgan@lmco.com	301.892.0710

ManTech	Paul Kuttner	BPA PM	paul.kuttner@mantech.com	571.216.1766
	Jeryl Ann Van Vleet	BPA Contract Manager	jeryl.vanvleet@mantech.com	703.873.6513
MicroTech	Zack Orchant	Director, IDIQ Programs	cdmcmaas@microtech.net	571.327.2903
	Jeannine Willingham	IDIQ Specialist	jwillingham@microtech.net	571.730.4036
Northrop Grumman	Dave Frederickson	CDM BPA Program Manager	dave.frederickson@ngc.com	703.883.8635
	Beverly Cenname	CDM Account Manager	beverly.cenname@ngc.com	703.399.1296
	CDM BPA Contracts Management	CDM BPA Contracts Management	cdm@ngc.com	703.556.1336
SAIC	Crystal Hrusovsky	Sr. Contracts Representative	crystal.m.hrusovsky@leidos.com	703.676.1566
	Patricia Presely		patricia.m.presely@saic.com	703.676.8016
			CDMBPA@leidos.com	
SRA	Todd Morris	Program Manager	todd_morris@sra.com	703.803.1823
	Nick Murray	Business Developer	nick_murray@sra.com	703.284.3290
	Art De Los Santos	Contracts Manager	art_delossantos@sra.com	703.322.4931
Technica	Paul Gentry	Contracts Manager	pgentry@technicacorp.com	703.662.2042
	Helen Kelly	CDM Program Manager	hkelly@technicacorp.com	703.662.2121
	Jim Sutton	DHS Account Lead	jsutton@technicacorp.com	703.662.2076
	Tabitha Fletcher	Contracts Administrator	tfletcher@technicacorp.com	703.662.2052