Sample Order Under

The Contractor's Basic GSA Schedule contract is applicable to the Order that is awarded under this BPA

ISSUED BY:
General Services Administration
Federal Systems Integration and Management Center (FEDSIM)
2100 Crystal Drive
Suite 800
Arlington, VA 20406

January X, 2012

ORDER REQUEST FOR QUOTE (RFQ)

SAMPLE Order: 001

Blanket Purchase Agreement
CDM Implementation Sample

in support of:

The U.S. Department of Homeland Security

NOTE: Section 1 of the BPA is applicable to this RFQ and is hereby incorporated by reference. In addition, the following applies:

1.1. GENERAL DESCRIPTION

The contractor shall perform some portions of the effort required by this sample order (SO) on a firm fixed price (FFP) basis/Labor Hour (LH) basis. The work shall be performed in accordance with all sections of the blanket purchase agreement (BPA), this order and the contractor's GSA Schedule.

1.2. SERVICES AND PRICES/COSTS

The following abbreviations are used in this price schedule:

CLIN:	Contract Line Item Number
LH:	Labor Hour
NTE:	Not to Exceed

1.2.1 BASE PERIOD:

FFP CLINs

CLIN	Description	QTY	Unit	Total Firm Fixed Price
0001	CDM Tools		User	$

Tools	Unit	Qty	Unit Price	Total Price
Contractor to Propose				
TOTAL PRICE				

CLIN	Description	QTY	Unit	Total Firm Fixed Price
0002	Labor (SO Task 1)	1(12)	Lot (Month)	$

LH CLIN

CLIN	Description	Total Hours	Total NTE Ceiling
0003	Labor (SO Task 2)		

Labor Category	Hours	Hourly Rate
Contractor to Propose		
TOTAL HOURS		

TRAVEL CLIN

CLIN	Description		Total Not-to-Exceed Price
0004	Travel	NTE	$ 2,500

GRAND TOTAL ALL CLINs **$________________**

1.2.2 OPTION PERIOD ONE:

FFP CLINs

CLIN	Description	QTY	Unit	Total Firm Fixed Price
1001	CDM Tools		User	$

Tools	Unit	Qty	Unit Price	Total Price
Contractor to Propose				
TOTAL PRICE				

CLIN	Description	QTY	Unit	Total Firm Fixed Price
1002	Labor (SO Task 1)	1(12)	Lot (Month)	$

LH CLIN

CLIN	Description	Total Hours	Total NTE Ceiling
1003	Labor (SO Task 2)		

Labor Category	Hours	Hourly Rate
Contractor to Propose		
TOTAL HOURS		

TRAVEL CLIN

CLIN	Description		Total Not-to-Exceed Price
1004	Travel	NTE	$ 2,500

GRAND TOTAL ALL CLINs **$________________**

1.2.3 OPTION PERIOD TWO:

FFP CLINS

CLIN	Description	QTY	Unit	Total Firm Fixed Price
2001	CDM Tools		User	$

Tools	Unit	Qty	Unit Price	Total Price
Contractor to Propose				
TOTAL PRICE				

CLIN	Description	QTY	Unit	Total Firm Fixed Price
2002	Labor (SO Task 1)	1(12)	Lot (Month)	$

LH CLIN

CLIN	Description	Total Hours	Total NTE Ceiling
2003	Labor (SO Task 2)		

Labor Category	Hours	Hourly Rate
Contractor to Propose		
TOTAL HOURS		

TRAVEL CLIN

CLIN	Description		Total Not-to-Exceed Price
2004	Travel	NTE	$ 2,500

GRAND TOTAL ALL CLINs **$________________**

2. TASKS AND ACTIVITIES UNDER THIS ORDER

2.1 PURPOSE

The purpose of this order is to support the United States (U.S.) Department of Homeland Security (DHS), National Cyber Security Division, in providing Continuous Monitoring Diagnostics Support for BPA GSC-QF0B-13-32662-0001. This order is for the planning, provisioning, configuration, operation, and management of tools, sensors, and dashboards to support Continuous Monitoring Diagnostics for multiple federal departments and agencies as described below. It is also for training for these departments and agencies in the integration of continuous monitoring tools in their information system (IS) security risk management processes, using the results of continuous monitoring for the reduction of risk through the prioritized mitigation of serious defects in IS security posture.

2.2 CHARACTERISTICS OF COVERED AGENCY NETWORK INFRASTRUCTURE COMPONENTS

The federal agencies that are the subject of this SO (referred to as SO Agency A, B, C, D, E, and F) include one agency with approximately 110,000 covered devices, and five smaller agencies with devices numbering from approximately 6,000 to just 100. The total of all covered devices is approximately 120,000.

Covered network-connected hardware devices by type for all SO Agencies:

End User Computing Platforms, by operating system	Windows XP: 70%, Windows 7: 15%, Windows Vista: 5%
Server Platforms, by operating system	Windows 2008: 5%, Windows 2003: 2%, Windows 2000: 1%, Unix/AIX: 1%, Linux: 0.5%, Sun Solaris: 0.5%.

For purposes of estimating, 7% of covered devices are server platforms.

SO Agency A:
Number of covered devices: 110,000
Number of user accounts: 1,100 privileged account, 120,000 regular accounts
Number of agency personnel requiring training: 700
Primary data center location: Arlington, VA

SO Agency B:
Number of covered devices: 6,000
Number of user accounts: 150 privileged account, 10,000 regular accounts
Number of agency personnel requiring training: 100
Primary data center location: Washington, D.C.

SO Agency C:
Number of covered devices: 1,000
Number of user accounts: 50 privileged accounts, 1,200 regular accounts
Number of agency personnel requiring training: 30

Primary data center location: Washington, D.C.

SO Agency D:
Number of covered devices: 100
Number of user accounts: 10 privileged accounts, 120 regular accounts
Number of agency personnel requiring training: 5
Primary data center location: Washington, D.C.

SO Agency E:
Number of covered devices: 1,000
Number of user accounts: 50 privileged accounts, 1,200 regular accounts
Number of agency personnel requiring training: 25
Primary data center location: Kansas City, MO

SO Agency F:
Number of covered devices: 2,000
Number of user accounts: 100 privileged accounts, 2,400 regular accounts
Number of agency personnel requiring training: 50
Primary data center location: Atlanta, GA

2.3 SO TASK 1, PROGRAM MANAGEMENT

The contractor shall provide Continuous Diagnostics and Mitigation (CDM) support for this SO issued according to the requirements and standards of the BPA and those provided below.

The contractor shall provide all necessary personnel, administrative, financial, and managerial resources necessary for the project management support of this SO. This includes the management and oversight of the SO work performed by contractor personnel, including subcontractors, to satisfy the requirements identified in the SO. The contractor shall identify a Program Manager (PM) by name, designated as Key Personnel, who shall serve as the primary interface and point of contact with the Government program authorities and representatives on SO management and technical project issues.

The contractor shall institute and maintain a management process that shall manage work efforts to accomplish the requirements of the SO and oversee all contractor personnel, Government-provided equipment, security matters, and financial resources utilized in performing this SO. The contractor’s Project Manager for SO tasks must be proactive and responsive to managing contractor resources and meeting DHS and other customer agency requirements.

The contractor shall notify the Contracting Officer (CO), Federal Systems Integration and Management Center (FEDSIM) Contracting Officer Representative (COR) and DHS Government Technical Point of Contact (TPOC) of any technical, financial, personnel, or general managerial problems encountered throughout performance of SO. The contractor shall prepare a Problem Notification Report (PNR), using the contractor’s format, to present to the COR and TPOC and to report details and impact of any such problems (see Section 5.6, Deliverable 08).

2.3.1 SO TASK 1, SUBTASK 1 –PROGRAM KICKOFF MEETING

The contractor shall schedule and coordinate a Program Kick-Off Meeting (see Section 5.6, Deliverable 01) at the Government's site. At a minimum, the attendees shall include key contractor personnel, representatives from DHS, other key Government personnel, the CO, the COR, and the DHS Government TPOCs from each of the sample agencies. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the SO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization, and reporting procedures. At a minimum the contractor shall discuss the following:

a. Draft Project Management Plan (PMP)
b. Draft Work Breakdown Structure and Initial Project Schedule
c. Contractor proposed performance metrics
d. Security requirements
e. Government-furnished information
f. Monthly meeting dates
g. Invoicing procedures
h. Points of contact
i. Roles and responsibilities
j. Order transitioning process and timeframes
k. Prioritization of contractor activities
l. Quality surveillance

The contractor shall prepare and deliver a Program Kick-off Agenda (see Section 5.6, Deliverable 02) that includes at a minimum the above referenced items. The contractor shall prepare and deliver a Program Kick-off Report (see Section 5.6, Deliverable 03) that documents the results of the meeting. Finally, the contractor shall prepare and present the draft Project Management Plan, including the draft WBS, proposed performance metrics, and initial project schedule (see Section 5.6, Deliverable 09).

2.3.2 SO TASK 1, SUBTASK 2 –SAMPLE ORDER MANAGEMENT MEETINGS/REPORTS

The contractor's SO Project Manager shall meet with the FEDSIM COR and DHS TPOC weekly for the duration of the SO to evaluate and track progress of contract performance measures. The contractor shall prepare an SO Meeting Agenda (see Section 5.6, Deliverable 04) to include, but not be limited to, contract costs and billings, performance period and schedule, activities, outstanding action items, and risks,. The contractor shall also prepare and distribute SO Meeting Minutes (see Section 5.6, Deliverable 05).

The contractor shall develop and submit a Monthly Progress Report (see Section 5.6, Deliverable 06) to the FEDSIM COR and DHS TPOC. The contractor shall deliver these reports to all appropriate parties identified by the Government.

2.3.3 SO TASK 1, SUBTASK 3 – COMPLETE AND MAINTAIN PROJECT MANAGEMENT PLAN

The contractor shall complete a final PMP (see Section 5.6, Deliverable 10), including WBS, project schedule, milestone dates, and performance metrics. The contractor shall update the plan as reqired to keep it current with actual and planned SO task progress.

2.3.4 SO TASK 1, SUBTASK 4 –TRIP REPORTS

As required the contractor shall provide, in the contractor's own format, a Trip Report (see Section 5.6, Deliverable 07) that summarizes all long-distance travel for work under this order, to include, at a minimum, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

2.4 SO TASK 2—CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) SYSTEM AND SECURITY ENGINEERING SERVICES

The sub-activities below shall be performed by the contractor as required at the order level. The contractor shall provide this support in accordance with the terms of the BPA, and requirements of this SO.

2.4.1 SO TASK 2, SUBTASK 1 – CDM ORDER PLANNING

The contractor shall provide plans describing their proposed approach to implementing the specific CDM capabilities required by the SO. The goal of the Order Planning activity is to integrate the contractor's CDM methodologies and best practices, into a sufficiently detailed plan, to ensure successful implementation and operation of the CDM capabilities required by the SO. The contractor shall provide the following documentation under this sub-task.

a. Continuous Monitoring as a Service (CMaaS) SO System Implementation Architecture (see Section 5.6, Deliverable 11). The contractor's solution architecture for providing hardware asset management (HWAM), software asset management (SWAM), configuration management (CM), and vulnerability management (VUL), in accordance with the CDM Tools and CMaaS BPA, Section 9, Attachment N. The solution architecture shall show sensors, dashboards, and connectivity for each of the six SO Agencies A – F. The planned architecture shall include consideration for:

    1) Support of economies of scale in implementing the required services across the multiple D/As.
    2) Support for SO Agencies A, B, and C that require dashboard and sensors to be located on the same network being analyzed without imposing substantial extra costs for such co-location. SO agencies D, E, and F do not have this co-location requirement.
    3) Implementing architectures for a range of sizes and types of organizations and demonstrate the benefits of a flexible architecture to meet unique federal agency requirements.
    4) Methodologies to implement CDM that would improve performance of CDM tools and minimize impact to the target IT network.

5) How the solution will meet the requirements of the HWAM function (see Section 9, attachment N of the CDM Tools and CMaaS BPA). Plan to include:

    i. Discussion of how the solution addresses each operational and functional requirement of the HWAM area, see Section 9, Attachment N of the CDM Tools and CMaaS BPA, Section 1.4, and all sub-paragraphs.
    ii. Discussion of how removable devices shall be reported, including when they are disconnected from the network.
    iii. The level of expected coverage of devices in terms of a percentage.
    iv. Description of method(s) for populating inventories.
    v. What details of hardware devices will be captured by the solution including any property management information such as owners, users, machine name, etc.
    vi. Description of how the solution will allow users to locate hardware on the network.
    vii. Discussion of what options the solution will support for scheduling hardware detection and who can control this process.
    viii. Discussion of the contractors proposed method for getting authorized user feedback on the accuracy of inventory data.
    ix. Discussion of how the HWAM tool(s) will interoperate with other systems. What data may be used and / or be made of available from / to the HWAM tool(s). What data standards are supported (e.g., extensible markup language (XML)-based security content automation protocol (SCAP) or National Institute of Standards and Technology (NIST)-specified open standards). Also how HWAM data will be stored.
    x. If applicable, any other HWAM features or functions, in addition to those in the requirements, that the contractor feels will provide relevant benefit to the Government and the SO Agencies.

6) How the solution will meet the requirements of the SWAM function (see Section 9, Attachment N of the CDM Tools and CMaaS BPA). Plan to include:

    i. Discussion of how the solution addresses each operational and functional requirement of the SWAM area, see Section 9, Attachment N of the CDM Tools and CMaaS BPA, Section 2.4, and all sub-paragraphs
    ii. Discussion of software identifying characteristics captured by the contractor’s solution. Including recommended considerations for detecting mobile and resident executable code.
    iii. Discussion of the contractor’s solution’s ability to capture software property management and accounting information (i.e., owner, data acquired, software keys, etc.), and / or recommended approach to capturing / managing this data.
    iv. Description of method(s) for populating inventories, including automatic and manual methods.

v. Discussion of what options the solution will support for scheduling software detection, and who can control this process.

vi. Description of how the solution will allow users to locate software on the network.

vii. Detailed discussion of how malware will be managed by the solution. Including identification of different types (e.g., Trojan horse, adware, polymorphic virus) if Malware Attributes Enumeration and Characterization (MAEC™) or Common Attack Pattern Enumeration and Classification (CAPEC™) is used. Any options for removal.

viii. Discussion of the management of software white list functions, and any labor saving approaches the contractor's solution may support for white listing software.

ix. Discussion of how the solutions will block unauthorized resident software and if mobile executables will also be blocked.

x. Discussion of the contractor's proposed method for getting authorized user feedback on the accuracy of inventory data.

xi. Discussion of solution for synchronizing SWAM inventories with CM and VUL functions.

xii. Discussion of how inventory data can be used from LDAP or property management systems, and if this can be used to validate attributes of authorized software.

xiii. Discussion of how the SWAM tool(s) will interoperate with other systems. What data may be used and / or be made of available from / to the SWAM tool(s). What data standards are supported (e.g., XML-based SCAP, or NIST-specified open standards). Also how SWAM data will be stored.

xiv. Discussion of how the tool administrator may assign users access to the tool, by groups or control groups.

xv. If applicable, any other SWAM features or functions, in addition to those in the requirements, that the contractor feels will provide relevant benefit to the Government and the SO Agencies (e.g., interface capabilities to provide network mapping / design data, trend analysis, compliance reporting, assignment of risk values, property management features).

7) How the solution will meet the requirements of the CM function (see Section 9, Attachment N of the CDM Tools and CMaaS BPA). To include:

i. Discussion of how the solution addresses each operational and functional requirement of the CM area, see Section 9, Attachment N, of the CDM Tools and CMaaS BPA, Section 3.4 and all sub-paragraphs.

ii. Discussion of how the CM solution addresses changes to the authorized security baseline.

iii. Discussion of the contractor's proposed solution for CM functionality for non-networked IT assets.

iv. Discussion of how the CM tool(s) will interoperate with other systems. What data may be used and / or be made of available from / to the SWAM tool(s). What data standards are supported (e.g., XML-based SCAP, NIST-specified open standards, Extensible Configuration Checklist Definition Format (XCCDF), Open Vulnerability Assessment Language (OVAL®), asset reporting format (ARF) or asset summary reporting (ASR)). Also how CM data will be stored.

v. Discussion of how users can maintain risk vulnerability scores for each vulnerability setting within a security configuration benchmark.

vi. Discussion of how data on misconfigured assets can be made available to the HWAM, SWAM, and VUL functions.

vii. If applicable, any other CM features or functions, in addition to those in the requirements, that the contractor feels will provide relevant benefit to the Government and the SO Agencies

8) How the solution will meet the requirements of the VUL function (see Section 9, Attachment N of the CDM Tools and CMaaS BPA). Plan to include:

i. Discussion of how the solution addresses each operational and functional requirement of the VUL area, see Section 9, Attachment N of the CDM Tools and CMaaS BPA, Section 4.4, and all sub-paragraphs.

ii. Discuss how the solution will help prioritize what to problems to fix first. The contractor shall discuss methodology the tool(s) use to determine the scoring of weaknesses.

iii. Discussion of how vulnerabilities shall be detected and reported for USB removable devices.

iv. Discussion of how grouping and hierarchical categorization of vulnerabilities shall work within the solution.

v. Discussion of how the tool supports migration to the desired state, through text-based instructions to system administrators or through automated means.

vi. Discussion of how the VUL tool(s) will interoperate with other systems. What data including user defined data, that may be used and / or be made of available from / to the VUL tool(s). What data standards are supported (e.g., XML-based SCAP, NIST-specified open standards, ASR, software identification (SWID) Tag data standard as defined in ISO/IEC 19770-2). Also how CM data will be stored.

vii. If applicable, any other VUL features or functions, in addition to those in the requirements, that the contractor feels will provide relevant benefit to the Government and the SO Agencies (e.g., interface capabilities to provide network mapping / design data, trend analysis).

9) Any other considerations the contractor believes to be relevant.

b. Security Model and Accreditation package (see Section 5.6, Deliverable 12), describing the contractor’s plan for implementing required security controls and its security model to prevent cross-propagation of malware across requesting organizations. For each of the SO agencies, the Security Model and Accreditation package shall:

1) For SO Agency B, propose at least one security model to protect the CDM data on both UNCLASS High Impact systems and CLASS systems through Top Secret, which has a high likelihood of being acceptable to DAAs in all civilian federal agencies.
2) Proposes such a model for several architectures which support flexibility in where to locate the sensors and tools.
3) Propose a security model that includes access controls to be applied to provide separate data views to each SO agency's organizational levels and roles based on their level and scope of responsibility.
4) Propose an approach to security that is technically designed to balance the cost of security with the benefits, including providing adequate security for the architecture that best allows the contractor to provide economies of scale in implementing the work under this vehicle.
5) Propose a security model that shows how the contractor will support security control assessment to enable DHS and the customer agencies to perform system security authorization as described in the NIST Risk Management Framework.
6) Propose a security model that includes applying continuous monitoring capabilities (HWAM, SWAM, VUL, CONFIG) to the IT components of the CDM solution itself.
7) Propose innovative ways to improve security performance.

c. Concept of Operations (see Section 5.6, Deliverable 13),

d. Plan for Transition to Production Operations (see Section 5.6, Deliverable 14) from the existing architecture, including integrating existing tools and dashboards (SO Agencies D, E, and F have existing dashboards). Considering all of the SO agencies the Transition Plan shall include:

1) Methodology for converting large quantities of data (comparable to 3 billion tests every 3 days) into useful information to support operational, tactical, and strategic decisions for SO agencies.
2) Methodology for integrating data from various COTS CM tools to support such decision systems for such customers, including managing technical refresh and upgrades of multiple products.
3) Developing methods to estimate threats, vulnerability and/or impact related to cyber-security, and using that information to drive wise risk acceptance decisions.
4) Using SCAP to integrate security sensor results.

e. Plan for Production Operations (see Section 5.6, Deliverable 15), describing how the provider will operate the proposed architecture to meet CDM objectives. For all of the SO agencies, the Operations Plan shall detail:

1) Operation of CDM installations for all six SO Agencies 500K devices, with SO Agency A having over 100K devices.
2) Collection of data on at least 95% of devices (or better) in each set of two successive scans.
3) Conduct of scans at least every seven days, with a goal of every three days.
4) Performance of effective and efficient technical refresh/version upgrades across large infrastructures.

f. Plan for Governance Support (see Section 5.6, Deliverable 16), describing how the provider will assist the six SO agencies to establish and coordinate governance of the CMaaS solution. The Governance Support Plan shall:

1) Detail a concept of operations to successfully train and/or mentor managers in all six of the SO agencies to successfully prepare, motivate, and/or enable their workforce to use information and automation to significantly improve their CDM performance.
2) Detail how CDM performance of the SO agency is linked to the workforce and how rewarding and empowerment of strong performers will be used to improve performance. Focus on positive incentives for improved performance and enabling factors, rather than on issuing orders and punishing non-compliance for imperfection
3) Detail how CDM trainers and consultants will be sourced to provide such training and mentoring.
4) Provide methods of change management to ease cybersecurity workers into higher performance, and motivating them by measuring progress along the way.

g. Requirements for any Government Furnished Equipment, CDM Tools, Government-provided information, or Government-Furnished Services (see Section 5.6, Deliverable 17) on which the provider is relying to meet the SO requirements.

2.4.2 SO TASK 2, SUBTASK 2 – INTEGRATE EXISTING DASHBOARDS AND REPORTING TOOLS

For Agencies, D, E, and F, who have existing dashboards / CDM reporting tools, the contractor shall integrate CDM data and operations into the existing systems.

2.4.3 SO TASK 2, SUBTASK 3 – PROVISION SPECIFIED TOOLS AND SENSORS

The contractor shall provision and configure a suite of sensors to perform diagnostics and monitoring of the target devices described in Section 2.2 for the following functions as described in Table 1: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, and Vulnerability Management.

Table 1. Security Diagnostic Capabilities within Scope of this SO

CDM Capability Description
1. **Manage hardware inventory**: Maintain an inventory of covered hardware assets, including to whom they are assigned for management, thereby providing system owners with a tool by which they can either remove unmanaged hardware from the inventory or assign it to someone for authorization and management. Hardware Inventory covers virtual machines (since they are individually addressable and behave like hardware on the network) as well as all physical devices on which software resides.
2. **Manage software inventory**: Maintain software inventories that reflect the authorized state (software is configured as released); the actual state (whether changes have been made); the difference, and to assign and control software so that integrity can be maintained. Software includes any executable code on hardware devices and includes firmware, Hardware Description Language (HDL) images, and the environment that allows the instantiation of virtual machines (e.g., VMWare) in addition to the more obvious operating systems, OS utilities, and applications. Prevent attackers from exploiting unauthorized software by ensuring
3. **Manage configuration settings**: Define an appropriate desired operational state for security configuration settings (including port, protocols, and services) and maintain it in operation. The Manage Configuration Settings capability addresses the modification of parameters that affect the underlying behavior of the software or hardware.
4. Manage vulnerabilities: Use the National Vulnerability Database (NVD) and other tools to find and remove exploitable vulnerabilities in software. This capability is to ensure that mistakes are identified and removed or remediated from operational systems faster than they can be exploited.

2.4.4 SO TASK 2, SUBTASK 4 – CONFIGURE AND CUSTOMIZE TOOLS AND SENSORS

The contractor shall, according to the requirements of SO Agencies A - F, 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 SO Agency to:

a. Record the desired state for authorized assets.
b. Specify its own categories for grouping results.
c. Customize scoring algorithms to quantify results.
d. Customize grading standards for defect scores.
e. Establish responsibility for maintaining the desired state (and mitigating defects) of each assigned and discovered asset.

Data integration requirements are estimated at 3 billion test results per discovery/scanning cycle (3 days) for the target population of covered devices described in Section 2.2.

2.4.5 SO TASK 2, SUBTASK 5 –MAINTAIN DESIRED STATE OF TOOLS AND SENSORS

The contractor shall provide operational capability for the installed, configured tools and sensors to enable SO Agencies to keep the data current for the desired state of target IT assets, as needed, on an ongoing basis.

2.4.6 SO TASK 2, SUBTASK 6 –SUPPORT INDEPENDENT VALIDATION AND VERIFICATION (IV&V) OF INSTALLED CDM TOOLS

The Government will conduct independent validation and verification (IV&V) of the installed CDM tools and architecture. The contractor shall provide all necessary data, documentation, and support for IV&V efforts.

2.4.7 SO TASK 2, SUBTASK 7 – OPERATE TOOLS AND SENSORS

The contractor shall operate the installed suite of CDM sensors to determine and report the actual state for functions defined in Table 1: Hardware Inventory Management, Software Inventory Management, Configuration Setting Management, Vulnerability Management, collecting monitoring data for all required conditions with coverage of 95% of devices (or better) in each set of two successive scans. Discovery scans and other data collection must be completed at least once every seven days for all covered devices, with a goal of every three days.

2.4.8 SO TASK 2, SUBTASK 8 – INTEGRATE AND MAINTAIN INTEROPERABILITY BETWEEN CDM TOOLS AND D/A LEGACY APPLICATIONS AND DATA

The contractor shall integrate CDM operated tools with associated SO Agency information systems (as specified in the SO) and maintain interoperability between the CDM tools and the SO Agency data in operation. (For example, an SO Agency might want to have data feeds exchanged between their existing property management system and the HWAM infrastructure.)

2.4.9 SO TASK 2, SUBTASK 9 – OPERATE DATA FEEDS TO AND FROM DASHBOARDS AND REPORTING SYSTEMS

The contractor shall operate the existing dashboard data feeds from the tools and sensors operated under Section 2.4.7 to the appropriate dashboard(s) and any requested reporting systems.

2.4.10 SO TASK 2, SUBTASK 10 – TRAINING AND MENTORING IN CDM GOVERNANCE FOR DEPARTMENTS, AGENCIES, AND OTHER REQUESTING ORGANIZATIONS

The contractor shall provide training and/or mentoring to SO Agencies A – F, in accordance with the contractor’s Government-approved CDM Governance Plan, to assist them in establishing an overall cybersecurity governance program with emphasis on using the continuous diagnostics to develop methods to estimate threats, vulnerability, and/or impact related to cyber-security, and using that information to drive rational risk acceptance decisions, perform the most cost-effective mitigations within available resources.

PACKAGING AND MARKING

NOTE: Section 3 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

NOTE: Section 4 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

NOTE: Section 5 of the BPA is applicable to this RFQ and is hereby incorporated by reference. In addition, the following applies:

5.1 PLACE OF PERFORMANCE

Place of performance is at the DHS headquarters building, 451 Seventh Street, SW, Washington, D.C. Occasional long distance travel may be required in support of this effort.

5.2 PERIOD OF PERFORMANCE

The period of performance for this SO is three years: one base year, plus two, one-year option periods starting at the date of award.

5.6 ORDER SCHEDULE AND MILESONE DATES

PS = Project Start is the same as order award date.
WD = Government Work Day

NUMBER	MILESONE/ DELIVERABLE	ORDER REFERENCE	PLANNED COMPLETION DATE
01	SO Kick Off Meeting	2.3.1	PS + 5 WDs
02	SO Kick-Off Agenda	2.3.1	PS + 3 WDs
03	SO Kick-Off Report	2.3.1	Order Kick Off + 3 WDs
04	Weekly SO Meeting Agenda	2.3.2	3 WDs before the Meeting
05	Weekly SO Meeting Minutes	2.3.2	2 WDs after the Meeting
06	Monthly Progress Reports	2.3.2	3 WDs before the BPA/Order Meeting
07	Trip Report	2.3.4	As required
08	PNRs	2.3	1 WD after Problem
09	Draft SO Project Plan including WBS, proposed performance metrics, and project schedule	2.3.1	PS + 5 WDs
10	Final SO Project Plans including WBS, proposed performance metrics and project schedule	2.3.3	3 WDs after Draft Comments
11	CMaaS SO Implementation Architecture Plan	2.4.1	IAW with the Government approved SO Project Plan
12	Security Model and Accreditation Package	2.4.1	IAW with the Government approved SO Project Plan
13	Concept of Operations	2.4.1	IAW with the Government approved SO Project Plan
14	Plan for Transition to Production Operations	2.4.1	IAW with the Government approved SO Project Plan
15	Plan for Production Operations	2.4.1	IAW with the Government approved SO Project Plan

NUMBER	MILESONE/ DELIVERABLE	ORDER REFERENCE	PLANNED COMPLETION DATE
16	Plan for Governance Support	2.4.1	IAW with the Government approved SO Project Plan
17	Resource Requirements	2.4.1	IAW with the Government approved SO Project Plan

5.7 MARKINGS FOR ELECTRONIC DELIVERY

Electronic copies shall be delivered via e-mail attachment. The contractor shall label each electronic delivery with the Order Number and Project Title in the subject line of the e-mail transmittal.

5.8 PLACE(S) OF DELIVERY

Originals of all deliverables and correspondence shall be delivered to the GSA COR identified in *Contract Administration Data*.

Copies of all deliverables shall also be delivered to the TPOC listed in *Contract Administration Data*.

5.9 NOTICE REGARDING LATE DELIVERY/ PROBLEM NOTIFICATION REPORT

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) as soon as it becomes apparent to the contractor, that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

NOTE: Section 6 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

NOTE: Section 7 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

7.1 SPECIALIZED DISCIPLINES

The contractor shall propose for the following Key Persons, (see Section 11.10.6.1.3 a and b, of the BPA RFQ) with their submission for the BPA. The contractor may propose additional Key Personnel.

a. Project Manager (PM)
b. Sensor and Dashboard Installation and Operations Architect
c. Data Management and Integration Manager
d. System Security Manager
e. Governance Training and Mentoring Manager

7.2 NON-KEY PM TEAM

The contractor shall provide a staffing plan with any additional non-Key Personnel that possess experience in assisting with management of government programs.

CONTRACT CLAUSES

NOTE: Section 8 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

LIST OF ATTACHMENTS

NOTE: Section 9 of the BPA is applicable to this RFQ and is hereby incorporated by reference.

This page is intentionally left blank.