TASK ORDER REQUEST (TOR)

47QFCA19R0012

Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Task Order (TO) Group F

in support of:

Department of Homeland Security (DHS)

Issued to:
all contractors under the General Services Administration (GSA) Alliant 2 Government wide Acquisition Contract (GWAC)
Multiple Award Contracts

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

November 15, 2019

FEDSIM Project Number HS01007

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for:

a. Mandatory Labor CLINs 0001, 1001, 2001, 3001, 4001, and 5001
b. Optional Labor CLINs 0002, 1002, 2002, 3002, 4002, and 5002

The contractor shall perform the effort required by this TO on a Cost Reimbursement Not-to-Exceed (NTE) basis for:

a. Long-Distance Travel CLINs 0003, 1003, 2003, 3003, 4003, and 5003
b. Tools CLINs 0004, 1004, 2004, 3004, 4004, and 5004
c. Other Direct Costs (ODCs) CLINs 0005, 1005, 2005, 3005, 4005, and 5005
d. CAF CLINs 0006, 1006, 2006, 3006, 4006, and 5006

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from the Washington, District of Columbia (D.C.) metro area. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 BASE PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
0003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
0004	Tools Including Indirect Handling Rate _____%	NTE	$16,730,000
0005	ODCs Including Indirect Handling Rate _____%	NTE	$875,000

CAF

CLIN	Description		Total Ceiling Price
0006	CAF	NTE	$100,000

TOTAL CEILING BASE PERIOD CLINs: $_____

B.4.2 FIRST OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
1003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
1004	Tools Including Indirect Handling Rate _____%	NTE	$21,200,000
1005	ODCs Including Indirect Handling Rate _____%	NTE	$1,085,000

CAF

CLIN	Description		Total Ceiling Price
1006	CAF	NTE	$100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: $_____

B.4.3 SECOND OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
2003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
2004	Tools Including Indirect Handling Rate _____%	NTE	$18,580,000
2005	ODCs Including Indirect Handling Rate _____%	NTE	$966,000

CAF

CLIN	Description		Total Ceiling Price
2006	CAF	NTE	$100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: $_____

B.4.4 THIRD OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
3003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
3004	Tools Including Indirect Handling Rate _____%	NTE	$15,916,000
3005	ODCs Including Indirect Handling Rate _____%	NTE	$850,000

CAF

CLIN	Description		Total Ceiling Price
3006	CAF	NTE	$100,000

TOTAL CEILING THIRD OPTION PERIOD CLINs: $_____

B.4.5 FOURTH OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
4003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
4004	Tools Including Indirect Handling Rate _____%	NTE	$16,500,000
4005	ODCs Including Indirect Handling Rate _____%	NTE	$875,000

CAF

CLIN	Description		Total Ceiling Price
4006	CAF	NTE	$100,000

TOTAL CEILING FOURTH OPTION PERIOD CLINs: $_____

B.4.6 FIFTH OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
5001	Labor (Tasks 1–8)	$	$	$

OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
5002	Labor (Task 9)	$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
5003	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	$40,000
5004	Tools Including Indirect Handling Rate _____%	NTE	$17,105,000
5005	ODCs Including Indirect Handling Rate _____%	NTE	$900,000

CAF

CLIN	Description		Total Ceiling Price
5006	CAF	NTE	$100,000

TOTAL CEILING FIFTH OPTION PERIOD CLINs: $_____

GRAND TOTAL ALL CLINs: $_____

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODCs costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of $XXX,XXX,XXX for CLINs __*__ through __*__ is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through_____(entered at award), unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of $***,***,*** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

See **Section J, Attachment C** - Incremental Funding Chart (Excel Spreadsheet).

B.7 AWARD FEE RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment D** – Draft Award Fee Determination Plan (Word document).

C.1 BACKGROUND

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. The DHS CDM Program strengthens the cybersecurity of civilian Government data and networks by providing cyber defense capabilities that deliver relevant, timely, and actionable information through dashboards at the agency and Federal levels. The cyber landscape in which Federal agencies operate is constantly changing and dynamic. Threats to the nation's information security continue to evolve and Government leaders recognize the need for a modified approach to protecting our cyber infrastructure. The CDM Program enables DHS, along with Federal agencies and state, local, regional, and tribal governments, to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical cybersecurity-related information, and enhance risk-based decision making at the agency and Federal enterprise levels. The CDM Program benefits participating agencies by helping to identify information security risks on an ongoing basis so that agencies can rapidly detect and then respond to information security events.

Congress established the CDM Program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. CDM provides Federal agencies with capabilities and tools to identify and prioritize cybersecurity risks based on potential impacts allowing cybersecurity personnel to mitigate the most significant problems first.

The CDM Program is organized by capabilities as identified below in Figure 1: CDM Capabilities.

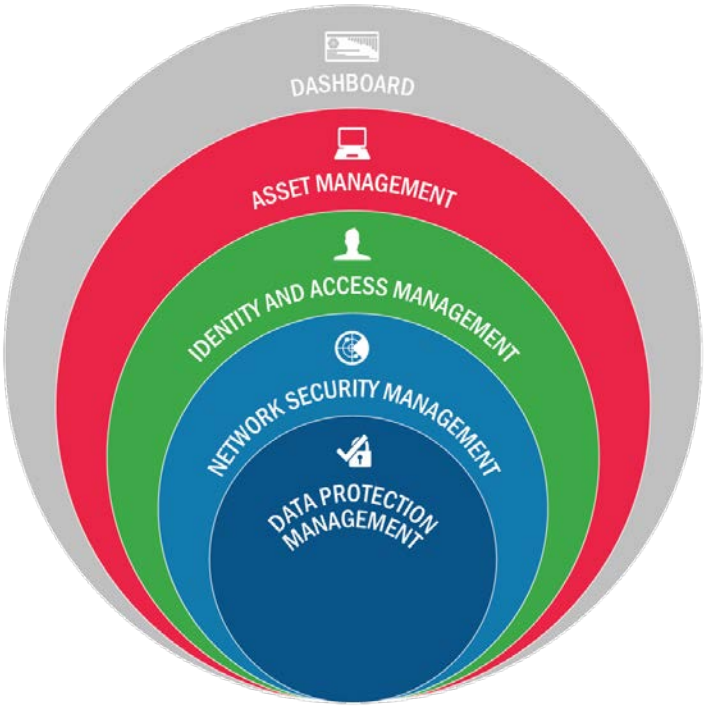

Figure 1: CDM Capabilities

The CDM Program provides cybersecurity tools, integration services, and dashboards to all participating agencies that enable them to improve their respective security postures. The CDM Dashboards, both Federal and agency, reinforce the CDM Program mission with an emphasis on the CDM Program's key tenant, which is to provide actionable information to allow agencies to "fix the worst problems first" across their Information Technology (IT) networks.

C.1.1 PURPOSE

The purpose of this TO is to provide DHS with a Shared Services Platform to provide CDM capabilities to supported Federal agencies. Additionally, this TO will provide a Shared Services Catalog (SSC) of capabilities and services that have been tested on the Shared Services Platform and found to be effective in meeting the goals of the CDM program. The SSC will be a continuously curated list that is intended to grow and change with the threat and technology landscape.

C.1.2 AGENCY MISSION

The CDM Program is managed within the DHS Cybersecurity and Infrastructure Security Agency (CISA) which is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. The DHS CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. DHS has been given the authority and Federal funding to implement the CDM Program to ensure that the approach to continuous monitoring is consistent and meets a common set of capabilities.

C.2 SCOPE

The previous CDM TO for Group F, TO2F, established the Shared Services Platform 1.0 and implemented initial CDM capabilities. These capabilities were formerly known as CDM Phases 1 and 2 but are now the Asset Management and Identity and Access Management Capabilities. The CDM DEFEND F procurement will expand the CDM services to those formerly known as Phases 3 and 4, but now referred to as the Network Security Management and Data Protection Management Capabilities. These capabilities are identified in the CDM Technical Capabilities Volume Two Requirements Catalog (**Section J Attachment J**). These capabilities will be provided by establishing a new Shared Services Platform 2.0, with an increased number of security services. CDM DEFEND F will then establish a SSC on the Shared Services Platform 2.0, which will be a managed collection of CDM capabilities that will be available for supported agencies to use. This DEFEND F TO is intended to support all current and future non-Chief Financial Officer (non-CFO) Act agencies. As of the release of this TOR there are 73 agencies that are either being supported, or are planned to be supported (see **Section J Attachment AA)**. The initial CDM capabilities targeted for inclusion in the SSC are identified in the CDM DEFEND F Initial SSC (**Section J Attachment BB**). Shared Services Platform 2.0 shall comply with the design guidance included in the CDM DEFEND F Shared Services Design Guidance and Conceptual Architecture document (**Section J, Attachment CC**). As part of DEFEND F, the SSC will be expanded to cover all CDM capabilities. The SSC will also require the contractor to

develop innovative solutions to the CDM capabilities that prioritize cloud native and hosted service solutions. To ensure continuity of services, the contractor shall operate the Shared Services Platform 1.0 after the current TO2F contract expires, up until the point that all supported agencies have been moved to the Shared Services Platform 2.0. The contractor shall coordinate all Authority to Operate (ATO) requirements for the Shared Services Platforms 1.0 and 2.0 and the CDM capabilities hosted by the platforms for supported agencies.

C.3 CURRENT IT/NETWORK ENVIRONMENT

The current CDM Shared Services TO2F Solution provides participating agencies (approximately 75 total Non-Chief Financial Officers (CFO) Act agencies) a Shared Services Platform 1.0 that extends CDM capabilities into a delivery model that adheres to the concepts of a shared service. The current environment is limited to CDM capabilities under "Asset Management" and "Identity and Access Management." The Shared Services Design Guidance is at **Section J, Attachment CC**.

C.4 OBJECTIVE

The objectives of this TO are to enhance the cybersecurity of participating agencies through the development and implementation of the Shared Services Platform 2.0 and the SSC. Specific objectives are to:

a. Facilitate agency adoption of CDM capabilities through the Shared Services Platform and the SSC.
b. Provide CDM shared services on an existing Federal Risk and Authorization Management Program (FEDRAMP) high rated Government cloud based platform
c. Establish a dynamic SSC that will grow with Government cybersecurity needs and adapt to changes in the cyber threat environment.
d. Move agency users from the Shared Services Platform 1.0 to the Shared Services Platform 2.0 without gaps or loss of CDM capabilities or services.
e. Operate the Shared Services Platform 1.0 until all agencies are moved to the Shared Services Platform 2.0.
f. Achieve the most advantageous cost and price discounts while provisioning agencies with CDM tools and capabilities

C.5 TASKS

Task 1: Provide Program Management
Task 2: TO Transition-In
Task 3: TO Transition-Out
Task 4: Design the Shared Services Platform 2.0
Task 5: Build, Test, and Secure the Shared Services Platform 2.0
Task 6: Integrate Agencies on the Shared Services Platforms 1.0 and 2.0
Task 7: Operate Shared Services Platforms 1.0 and 2.0
Task 8: Stakeholder Engagement
Task 9: (Optional) Provide SOC Services to the Shared Services Platform 2.0

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting **(Section F, Deliverable 03)** at a location approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, the DHS Technical Point of Contact (TPOC), other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR).

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 01**) for review and approval by the COR and the DHS TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties.
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Staffing Plan and status.
d. Overview of technical approach.
e. Transition-In Plan (**Section F, Deliverable 09**) and discussion.
f. Security discussion and requirements (i.e., building access, badges, Personal Identity Verification (PIV)).
g. Invoicing requirements.
h. Quality Management Plan (QMP) (**Section F, Deliverable 04**).
i. Deliverable tracking throughout the project.
j. High-level project schedule for first 60 days.
k. Agency onboarding tracking (**Section F, Deliverable 05**)
l. Project Management Plan (PMP) (**Section F, Deliverable 10**)
m. Master Repository Inventory format (**Section F, Deliverable 15**)
n. Financial reporting format (**Section F, Deliverable 16**)
o. Shared Services Platform 1.0 Take Over Plan (**Section F, Deliverable 42**)
p. Cutover Work Plan (CWP) (**Section F, Deliverable 35**)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (**Section F, Deliverable 02**) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (**Section J, Attachment F**) (**Section F, Deliverable 06**). The MSR shall include the following:

a. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
g. Cost incurred by CLIN.
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

C.5.1.3 SUBTASK 1.3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting (**Section F, Deliverable 07**) with the DHS TPOC, COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR (**Section F, Deliverable 08**).

C.5.1.4 SUBTASK 1.4 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP and shall provide it to the Government (S**ection F, Deliverable 10**).

The PMP shall contain:

1. Communications and stakeholder management (including the contractor's organizational chart and lines of authority). Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
2. Scope management
3. Requirements management.
4. Configuration management.

5. Staffing management.
6. Supply chain risk management to include procurement and logistics.
7. Risk management.
8. Cost management.
9. Standard Operating Procedures (SOPs) for all Section C tasks.

The PMP is an evolutionary document that shall be updated annually at a minimum and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.5 SUBTASK 1.5 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (**Section F, Deliverable 13**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in (**Section J, Attachment G**).

C.5.1.6 SUBTASK 1.6 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor's QMP (**Section F, Deliverable 04**) shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

The contractor's quality control shall be inclusive of the data being ingested through the agency and federal dashboard from supported agency tools and sensors.

The QMP shall include, but not be limited to, the following:

a. Performance monitoring methods.
b. Performance measures.
c. Approach to ensure that cost, performance, and schedule comply with task planning.
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO.
e. Government roles.
f. Contractor roles.

The contractor shall periodically update the QMP as changes in program processes are identified.

C.5.1.7 SUBTASK 1.7 – PREPARE MEETING REPORTS

The contractor shall conduct, attend, and participate in various project- and program-related meetings. These meetings may include, but are not limited to, Integrated Project Team (IPT) brainstorming sessions, program management reviews, technical status reviews, document reviews, and TO status reviews.

The contractor shall submit Meeting Reports **(Section F, Deliverable 14)** as requested by the COR and/or DHS TPOC to document meeting results and action items with owners. The Meeting Reports shall include the following information:

a. Meeting attendees and their contact information; at a minimum, identify organizations represented.
b. Meeting dates.
c. Meeting location.
d. Meeting agenda.
e. Purpose of meeting.
f. Summary of events (issues discussed, decisions made, and action items assigned).

C.5.1.8 SUBTASK 1.8 – PROVIDE FINANCIAL REPORTING

The contractor shall provide a Financial Report of cumulative expenditures monthly (**Section F, Deliverable 16)** to the COR and DHS TPOC. The Financial Report shall include at a minimum:

a. Monthly expenditures (hours and dollars) by CDM Capability/Phase incurred to date for each task from the start of the period of performance.
b. Projected monthly expenditures and labor hours by task starting with the current month through the end of the period of performance.
c. Funds expended, anticipated, incurred, and remaining by CLIN.
d. Diagram reflecting funding and burn rate by month for the TO.
e. Cumulative invoiced amounts for each CLIN up to the previous month.
f. Monthly and cumulative cost incurred by task categorized by CDM capability area.
g. Identification of the funding source (CDM or Agency).
h. Actual current and cumulative dollars expensed for small businesses compared to Alliant 2 subcontracting goals.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting (Section C.5.1.1) for Government review. The Government will provide written approval of the proposed format via the COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on DHS CDM PMO needs. Any changes to the format will be requested in writing via the COR.

C.5.1.9 SUBTASK 1.9 - PROCUREMENT SERVICES, ASSET TRACKING, AND LOGISTICS

The contractor shall procure and track necessary CDM DEFEND F Shared Services Platform 1.0 and 2.0 hosting costs, Tools, and ODCs required under the TO. The contractor shall coordinate with the COR and DHS TPOC and initiate the procurements using the procedures in Section H.11. The contractor shall develop a Procurement Report (**Section F, Deliverable 17**) in accordance with the Procurement Report Template (**Section J, Attachment T**) for CDM DEFEND F procurements under the TO. The Procurement Report shall initially capture the planned procurement, and later be updated to capture the lifecycle of Delivery and Acceptance. The Procurement Report shall be a living document and shall be updated periodically throughout the TO and, at a minimum, for the following instances:

a. New RIPs or Consent to Purchase (CTP).
b. Proposed cost from RIPs or CTPs, actual cost of products purchased, and price comparison (CDM Tools Special Item Number (SIN) price comparison if available).
c. Cost savings to the Government (i.e., discounts).
d. Product dates of order, delivery, receipt of goods by the CDM DEFEND F stakeholder.
e. The date of expiration for tools that require renewal.
f. Identified changes in a planned procurement of CDM DEFEND F tools.

The contractor shall work collaboratively with the DHS TPOC and COR to manage property accountability, including the acceptance of software licensing, certificates, etc.

The contractor shall identify, track, and control licenses procured under the TO and those licenses provided by the Government during the TO period of performance. The requirement to define, track, and control licenses procured under the TO shall be on-line/remotely accessible through standard web browser to provide Government situational awareness and ensure compliance with applicable license terms and conditions. Asset and logistics services shall include licensing inventory management and the tracking of license transfer and receipts.

The contractor shall provide associated logistical services and inventory management functions to maintain and track equipment and software accountable under this TO, including all procured licenses.

C.5.1.10 SUBTASK 1.10 – CONDUCT QUARTERLY IN-PROGRESS REVIEW (IPR) MEETINGS

The contractor shall conduct a formal quarterly IPR (**Section F, Deliverable 43**) at a location agreed to by the Government. The IPR shall provide a forum for Government review of progress, planning, and issues related to TO performance. The contractor shall utilize the PMP in its discussion of TO performance. The IPR shall replace the Monthly Status Briefing Meeting for that month.

IPRs shall, at a minimum, include:

a. Program status overview.
b. Status of the CDM DEFEND F Solution.
c. Schedule by task.
d. Previous month and quarter activities by task.
e. Planned activities for next month and quarter by task.
f. Financial status, to include quarterly cost savings report on material and equipment purchases.
g. Status of risks and issues.
h. Actions required by the Government.

The contractor shall prepare the IPR Agenda (**Section F, Deliverable 18**), IPR Meeting Report (**Section F, Deliverable 36**), and presentation material. IPRs shall be conducted no less than quarterly. The IPR is historically attended by an average of seven to 15 stakeholders, including contractor personnel, COR, DHS TPOC, and other key Government stakeholders.

C.5.1.11 SUBTASK 1.11 – MAINTAIN AN INTEGRATED MASTER SCHEUDLE (IMS)

The contractor shall develop and maintain an IMS (**Section F, Deliverable 37**). The IMS shall include all work necessary across the project, with major tasks, milestones, and deliverables, and planned and actual start and completion dates for each task, subtask, and work package. The IMS shall be developed and maintained as noted in Section F.

The IMS is an evolutionary document that shall be updated with technical inputs and significant changes as required. Significant changes represent any alteration, modification, or adjustment to the CDM DEFEND F solution or program that affects cost or schedule.

The contractor shall reflect the Government's requirements in planning for all activities and the tailored DHS Systems Engineering Life Cycle (SELC) process reviews in the IMS. The IMS shall be submitted monthly. The contractor shall work from the latest Government-approved version of the IMS.

C.5.1.12 SUBTASK 1.12 – COORDINATE AND COMPLETE SELC REVIEWS

The contractor shall coordinate and complete each SELC review detailed in the DEFEND–F SELC Process Overview (**Section J, Attachment DD**) for each SELC gate.

C.5.2 TASK 2 – TO TRANSITION-IN

The contractor shall provide a Transition-In Plan (**Section F, Deliverable 09**) as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan No Later Than (NLT) ten calendar days after project start, and all transition activities shall be completed 80 calendar days after project start. The contractor shall assume full responsibility of Shared Services Platform 1.0 as defined in Subtask 7.1 by the end of this transition period. The contractor shall adhere to all requirements to maintain the Authority to Operate (ATO) by DHS for the Shared Services Platform 1.0 solution.

C.5.3 TASK 3 – TO TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within six months of Project Start (PS) (**Section F, Deliverable 19**). The contractor shall review and update the Transition-Out Plan in accordance with the schedule in Section F. The Government reserves the right to request revisions to the Transition-Out Plan as major modifications are made to the technical solution.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor–to-contractor coordination to ensure a seamless transition.
f. Schedules and milestones.

g. Actions required of the Government.
h. Identification and transfer of Government owned data and assets.
i. Technical information on the shared services platform, ATO, configurations, network connections, administrative data and any other information necessary for its operation.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.4 TASK 4 – DESIGN THE SHARED SERVICES PLATFORM 2.0

This task includes all planning and design efforts to initially establish the Shared Services Platform 2.0 and all future updates to the Shared Services Platform. To support the design activities, the contractor shall develop and maintain a Shared Services Platform Roadmap and Innovation Document that presents a detailed plan for the Shared Services Platform and corresponding SSC to meet the operational and functional requirements of the CDM Capabilities and provide secure federated agency access to those capabilities. The contractor shall conduct Analysis of Alternatives (AoAs) as directed by the Government to provide an in-depth analysis of potential Shared Services Platform upgrades. The contractor shall complete the Solution Design Review (SDR) (**Section F, Deliverable 22)** SELC Gate as defined in the DEFEND –F SELC Process Overview (**Section J, Attachment DD**) in this task. Additional updates to the Shared Services Platform shall result in the contractor updating relevant SDR artifacts and/or conducting additional SDR gate reviews. The contactor shall provide a robust requirements management process that provides clear traceability and visibility into the Shared Service Platform.

C.5.4.1 SUBTASK 4.1 -- SHARED SERVICES PLATFORM ROADMAP AND INNOVATION REFRESH

In order to ensure functionality of the Shared Services Platform is current with the ever changing cyber threat environment, the contractor shall continuously review the cyber threat landscape, the cybersecurity tool marketplace, and any changes or innovations based on the CDM program or industry cybersecurity best practices. Based on this analysis, the contractor shall compile and implement a Shared Services Platform Roadmap and Innovation Document (**Section F, Deliverable 23**). Initially, the Shared Services Platform Roadmap and Innovation Document shall identify any gaps between the current Agency environments and those CDM capabilities noted in the CDM DEFEND F Initial SSC (**Section J Attachment BB**) and address how the new Shared Services Platform will close those gaps. The Shared Services Platform Roadmap and Innovation Document shall contain changes to the SSC that are necessary to ensure that the Shared Services Platform meets the current cyber threat environment. The Shared Services Platform Roadmap and Innovation Document shall contain the following information at a minimum:

a. Planned upgrades for the Shared Services Platform with each upgrade introducing new functionality and services through the SSC. The initial platform shall provide the functionality addressed in the CDM DEFEND F Initial SSC (**Section J, Attachment BB**)

b. Identification of CDM Capabilities that are recommended by the contractor or Federal agency stakeholders for inclusion into the Shared Services Platform through the SSC.
c. CDM Agency Dashboard upgrade schedule. The contractor shall update the Agency Dashboard as soon as possible once new Dashboard versions are released.
d. Planned major and minor upgrades to the Shared Services Platform. Major releases represent larger scale changes to the Shared Service Platform; minor upgrades represent planned patching/hot fixing of the underlying technology.
e. Virtual infrastructure updates.
f. Any CDM tools or Ancillary equipment on the Shared Service Platform and/or the SSC that are expected to become obsolete within the next year, or are underperforming and require replacement.
g. Descriptive rationale for the selection of any new IT products or for the replacement of existing Shared Services Platform products. The contractor shall include considerations for Supply Chain Risk Management whenever selecting new IT products.
h. Innovations in IT products or methods that may be applicable to the Shared Services platform or supported user base.

The contractor shall refresh the Shared Services Platform Roadmap and Innovation Document on a monthly basis (**Section F, Deliverable 23**), or when directed by the COR.

The contractor shall schedule, coordinate, and host a Quarterly Shared Services Review Meeting of the Shared Services Platform Roadmap and Innovation Document. This meeting shall be held at a location approved by Government. The meeting shall include the DHS TPOC, the COR, and other Government stakeholders from DHS or supported agencies as approved by the DHS TPOC and COR. The purpose of the meeting shall be to review the Shared Services Platform Roadmap and Innovation Document. During the meeting, the contractor shall present recommended changes to the Shared Services Platform and/or the SSC. The contractor may recommend, or the Government may require, ad hoc Shared Services Platform Review Meetings, prior to the regular quarterly meeting if changes to the cyber threat environment or the CDM Program require it.

C.5.4.2 SUBTASK 4.2 – CONDUCT AoA

The Government plans to analyze the CDM Shared Services Platform periodically for potential improvements, enhancements, and other changes including, but not limited to, the incorporation of a new CDM capability in the SSC, virtual infrastructure changes, upgrading of new technology, or the addition of services into the SSC. The contractor shall perform and document an AoA (**Section F, Deliverable 25**) when directed by the Government. The contractor shall complete an initial AoA within sixty days after project start. The contractor shall provide an updated AoA every six months or sooner if directed by the Government. The purpose of this frequency is to enable consideration of the most current technologies or methodologies (**Section F, Deliverable 25**). Based on findings in these updates, the contractor shall recommend changes, if any, to the Shared Services Platform to keep the platform current. The contractor shall provide an initial basis of estimate of labor hours and schedule to complete each AoA.

The contractor shall analyze and document each approach, its alternatives, and rationale for the contractor's recommendations in a specific AoA. Anticipated topics that could require the generation of an AoA include, but are not limited to, the following:

a. Optimal cloud service model to meet the requirements of the Shared Services Platform and CDM capabilities in the SSC.
b. Incorporation of alternate architectures to best meet Shared Services Platform requirements.
c. Approach to support a new CDM Capability in the SSC through the CDM Shared Services Platform.
d. Augmentation of the existing CDM Shared Services Platform Architecture including multi-tenancy and federated access to the CDM capabilities within the Shared Service Platform.
e. Potential procurement of an additional Commercial Off-the-Shelf (COTS) product to be integrated into the CDM Shared Services Platform.

The contractor shall conduct and deliver AoAs that shall include, at a minimum, the following:

a. An analysis of desired requirements and the ability for the current CDM Shared Services Platform to support those requirements including, but not limited to, technology demonstrations, modeling and simulation, and market research.
b. Solutions that have the ability to meet desired requirements.
c. Report on the cost and benefit, performance impacts, engineering trade-offs such as technical solution performance, user experience and data currency impacts, cost/benefit analysis, schedule impacts, and technical feasibility of analyzed solutions.
d. Recommendation for approach to desired requirements. This shall include a rationale for the recommended approach and sound reasoning for the rejection of alternative options.
e. Summarized briefing of the recommended approach, with additional details from requirements above made available as appendices.
f. Strategy for agency cutover to new concept, including discussion of agency or service based approach.

The Government will determine the best solution based on the alternatives presented in the AoA. The COR will coordinate with the contractor when appropriate on the next course of action after the AoA results are reported to the Government. An AoA may result in changes to the Shared Services Platform, including the SSC, which would require the contractor to execute activities identified in an AoA.

C.5.4.3 SUBTASK 4.3 – DEVELOP A DETAILED DESIGN FOR THE SHARED SERVICES PLATFORM

The contractor shall complete the System Design Review (SDR) (**Section F, Deliverable 27**) SELC Gate and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**). The intent of the SDR is to provide all key Government stakeholders with a common understanding of the foundational solution design and architecture to accomplish all of the Government's operational requirements, needs, and expectations. The intent of subsequent SDR events, when initiated by the Government, is to provide complete transparency for upgrades/changes to the Shared Services Platform. Completion of the SDR gate review is only possible when the contractor has met all exit criteria defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**).

The artifacts required to complete the SDR shall include consideration for the following topics:

a. Graphical representations/diagrams of the Shared Service Platform configuration inclusive of the following technical components:
    1. All virtual infrastructure components (Software as a Service (SaaS), Platform as a Service (PaaS), Virtual Machines (VM), etc.) supporting the core platform.
    2. CDM Agency Dashboard.
    3. Virtual or non-virtual components that support CDM capabilities.
    4. Network Diagrams (e.g., Designs, Data Flows, etc.).
    5. Interface architecture and specifications.
    6. CDM data transport, data compression, and guaranteed delivery assurances.
    7. Agency Multi-tenancy design including federated single sign-on authentication and role-based access controls.
b. Deployment of the CDM Agency Dashboard, including any technology required for proper Agency Dashboard/Federal Dashboard communication (e.g., message queuing, data streaming, etc.) and integration between the CDM capabilities, data normalization platforms, and the CDM Agency Dashboard.
c. Integration with the CDM Federal Dashboard and provisions for data feeds/exchanging mechanisms.
d. Implementation Plan for initial CDM Capabilities as outlined in the CDM DEFEND F Initial SSC (**Section J, Attachment BB**).
e. Networking designs inclusive of things such as
    1. Boundary defenses (Intrudence Detection System / Intrudence Protection System (IDS / IPS), Firewalls, etc.).
    2. Domain Name System (DNS) servers.
    3. Trusted Internet Connection.
f. Identity Access Management (IAM) considerations including:
    1. Federated authentication designs inclusive of integration with Government-furnished Identity Provider.
    2. Role-based access controls to multi-tenant CDM capabilities including the Agency Dashboards.
    3. Public Key Infrastructure (PKI) considerations.
g. Data architecture, design, and specifications including:
    1. Tool/Integration alignment to the CDM Data requirements.
    2. Technical method to employ Containerization (e.g., Organizational Unit (OU), Federal Information Security Modernization Act (FISMA), etc.) within the solution.
    3. Approach to data segmentation and access control (e.g., due care of agency data within the solution, Role Based Access Control (RBAC), etc.).
    4. Encryption of data storage, data at rest, and data in transit (including any PKI/Certificate and symmetric key management based designs).
h. Operational Requirements.
i. Testing and quality management.
j. Platform and CDM tool administration and governance. Including:
    1. Change management procedures.

2. Tool introduction and update management.
3. Tool license management.
4. ATO update procedures.
5. Development management and iterative life-cycle.

k. Establishment of production, test, and development Shared Services Platform environments, including any IT hardware, software, or personnel requirements.
l. Establishment of a Security Operations Center (SOC) for monitoring and incident management and/or providing access to the DHS Enterprise SOC (ESOC). This is not meant to be an SOC for the supported DEFEND F agencies, but rather for providing SOC support to the Shared Services Platform.
m. Establishment of help desk support for the Shared Service Platform for Tiers I – III.
n. Plan for attaining an ATO, including milestone dates and resources needed.
    1. This plan shall include the overall security architecture of the Shared Services Platform:
        i. Security Controls and technologies (configurations thereof) implemented to maintain confidentiality, integrity, and availability of Shared Service Platform.
        ii. Monitoring approach.
o. A comprehensive list of software, hardware (if any), and service requirements to implement the design and plan.

The Government will review the SDR and approve the contractor's design and plan with comments or edits.

C.5.4.4 SUBTASK 4.4 – PROVIDE REQUIREMENTS MANAGEMENT SERVICES

The contractor shall manage, elicit, analyze, document, communicate, and validate Shared Services Platform requirements. The contractor shall ensure all Shared Services Platform requirements are approved by the Government prior to any building, development, and deployment. For CDM capabilities available on the Shared Services Platform through the SSC, the contractor shall ensure that traceability exists to the CDM Technical Capabilities Volume Two Requirements Catalog. The contractor shall ensure that Shared Service requirements are developed and refined incrementally through an iterative process of identifying needs, defining acceptance criteria, and prioritizing, developing, and reviewing the results of these actions. The contractor shall ensure that the Shared Services Platform requirements management process is effectively monitored, with activity logging and traceability between requirements development and testing, which will verify and validate that the Shared Service Platform and CDM capabilities available through the SSC are delivered to end user satisfaction.

C.5.5 TASK 5 – BUILD, TEST, AND SECURE THE SHARED SERVICES PLATFORM 2.0

The contractor shall build, test, and secure the Shared Services Platform and the software and processes necessary to maintain the SSC on the Shared Services Platform 2.0. The SSC is a dynamic listing of CDM capabilities that can be provided to Federal agencies using the Shared Services Platform 2.0.

The contractor shall ensure that the Shared Services Platform is sufficiently secured and receives an ATO. The contractor shall establish an SOC for the Shared Services Platform 2.0. The contractor shall support efforts for the environment to receive an ATO within the base period of the TO.

C.5.5.1 SUBTASK 5.1 – BUILD, TEST, AND PREPARE THE CDM SHARED SERVICES PLATFORM 2.0 FOR PRODUCTION

Following successful completion of an SDR, the contractor shall proceed to establish the CDM Shared Services Platform 2.0 in accordance with the Government reviewed SDR artifacts. The contractor shall purchase all software, hardware, and virtual infrastructure services needed for the Shared Services Platform and CDM Capabilities available in the SSC on behalf of the Government. The contractor shall provision cloud services and implement CDM capabilities based on the approach detailed in the SDR. These activities shall be completed each time the Shared Services Platform is upgraded, including with any updates to the SSC that result in changes to the Shared Services Platform.

The contractor shall complete the Solution Readiness Review (SRR) (**Section F, Deliverable 28**) SELC Gate and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**). The intent of the SRR is to validate that the Shared Services Platform and the CDM capabilities available in the SSC are ready for testing in the contractor's development environment. Completion of the SRR gate review is only possible when the contractor has met all exit criteria as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**).

The contractor shall support Government Independent Validation and Verification (IV&V) activities, and it shall assist with any additional Government operational and security-related assessments of the Shared Services Platform throughout the TO period of performance. The contractor shall allow DHS CDM Project Management Office (PMO) and/or its designated representatives (e.g., IV&V Team) to observe and/or participate in all developmental and/or operational tests and evaluations conducted by the contractor.

The contractor shall support test activities by providing Test Plans (**Section F, Deliverable 29**) and procedures, along with a test environment (Section C.5.5.4) capable of executing these plans, which outline how the contractor intends to provide evidence and/or demonstrations that targeted functionality was achieved in the release. The CDM Program Test and Evaluation Master Plan (TEMP) (**Section J, Attachment EE**) describes the CDM Program's planned test and evaluation activities over the Program's lifecycle and identifies test evaluation criteria. The contractor shall align testing activities with the CDM Program TEMP. The DHS CDM PMO and/or its designated representatives will observe and/or participate in developmental and/or operational tests and evaluations. The Government may conduct additional operational and security-related assessments of the CDM Shared Service Platform and the underlying CDM capabilities available through the SSC. The contractor shall complete an initial Test Readiness Review (TRR) (**Section F, Deliverable 30**) following successful completion of the SRR. The Government will provide the contractor with direction to proceed with planned testing activities if the criteria have been met per the checklist provided in the CDM IV&V strategy.

Following successful completion of the TRR, the Government will review the results of the current Shared Service Platform development to determine whether the platform and CDM

capabilities targeted for completion were implemented satisfactorily and are ready for production. The contractor shall complete the Production Readiness Review (PRR) (**Section F, Deliverable 31**) SELC Gate and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**). The intent of the PRR is to validate that the Shared Services Platform and CDM capabilities available in the SSC are ready for the production environment. Completion of the PRR gate is possible only after all exit criteria defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**) have been met.

Following completion of the PRR on the Shared Services Platform, the contractor shall concurrently complete the following three SELC Gate reviews for the Shared Services Platform and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**) for the following gates:

a. User Acceptance Testing TRR (**Section F, Deliverable 30**)
b. Operational TRR (OTRR) (**Section F, Deliverable 20**)
c. Operational Readiness Review (ORR) (**Section F, Deliverable 21**)

Completion of these gates is possible only after the contractor has met all exit criteria as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**).

C.5.5.2 SUBTASK 5.2 – SECURE THE SHARED SERVICES PLATFORM 2.0

The Shared Service Platform is a DHS asset. The Shared Services Platform and supported CDM Capabilities available through the SSC have been categorized for Federal Information Processing Standard (FIPS) 199 as High Confidentiality, High Integrity, and Moderate Availability. Upon initial development of the Shared Service Platform, the contractor shall ensure that the Shared Services Platform receives an ATO, and then ensure that the ATO is maintained throughout all future upgrades to the Shared Services Platform. The contractor shall ensure the Shared Service Platform maintains a system security authorization following the most recent revision of National Institute of Science and Technology (NIST) Special Publication (SP) 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations and DHS Sensitive Systems Policy Directive 4300A and related DHS or CISA security policies and guidance.

The contractor shall support CISA in conducting a security assessment of the Shared Services Platform through drafting of deliverables (e.g. System Security Plan (SSP)), providing artifacts and screenshots, and making system personnel available for interviews during the security assessment process. The Government desires that the ATO be completed within the base period of the TO. In support of the security accreditation process of the Shared Services Platform, the contractor shall:

a. Provide all the required documentation for the security authorization process (e.g., system description, system architecture, security control, etc.) (**Section F, Deliverable 32**). This could include generation of additional security documentation to satisfy NIST 800-53 and DHS 4300A requirements.
b. Remediate all security findings and create of Plans of Action and Milestones (POA&Ms) and/or waivers, as appropriate.
c. Ensure DHS and/or CISA security requirements are met including, but not limited to,

regular delivery of vulnerability scans, asset management activities, POA&Ms, and/or waiver remediation activities.

d. Develop documentation to achieve security authorization, in ongoing authorization format, reflecting agency specific control implementations (**Section F, Deliverable 33**).
e. Apply CDM capabilities to the Shared Service Platform and report to the CISA CDM Agency Dashboard.
f. Support, as required, a Government provided SOC or contractor-provided SOC, and incident response activities such as investigative, remediation, and removal tasks, as appropriate.
g. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.

For each Shared Services Platform upgrade, the contractor shall update the Security Authorization Package and deliver updates to include the following documents (**Section F, Deliverable 34**):

a. Update applicable SSPs and SOPs as necessary.
b. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.
c. Create new POA&Ms and/or waivers, update existing POA&Ms and/or waivers, and conduct remediation of findings
d. Support the CISA Infrastructure Change Request (ICR) process. This includes drafting the ICR documentation and Technical Notes with integrated or attached Security Impact Assessments (SIA).
e. Support, as required, a Government provided SOC or contractor provided SOC, and incident response activities such as investigative, remediation, and removal tasks, as appropriate.

C.5.5.3 SUBTASK 5.3 – DEVELOP SHARED SERVICES PLATFORM HOTFIXES

For each production version of the Shared Services Platform in an operational environment, the contractor shall develop Quick-Fix Engineering updates or “HotFixes,” as required. HotFixes may include, but are not limited to, incorporating minor changes such as patches for the system components (e.g., CDM capabilities tools, the CDM Agency Dashboard, messaging technology, and security patches) and/or urgent bug fixes for information exchange with the CDM Federal Dashboard. The level-of-effort to support a HotFix is typically less than the design and development support associated with a full Shared Service Platform upgrade. The contractor shall be prepared to proactively provide security patching for all Shared Service Platform components when needed.

The contractor shall build, and test the HotFix in the appropriate test environment. Within 24 hours of testing completion, the contractor shall move the HotFix to Operations and Maintenance (O&M) of the production version of the Shared Services Platform. The contractor shall update any necessary supporting documentation that is affected by a HotFix.

C.5.5.4 SUBTASK 5.4 - BUILD AND MAINTAIN A RESEARCH, DEVELOPMENT, TEST, AND EVALUATION (RDT&E) ENVIRONMENT

The contractor shall execute RDT&E activities in an environment that supports industry best practices. The RDT&E environment shall support, but is not limited to, the following activities:

a. All testing activities necessary for the shared services platform.
b. Research activities for future shared services platform changes.
c. Technology demonstrations, modeling, and simulation as part of an AoA.
d. SELC gate demonstrations
e. Operational upgrades (e.g. CDM Dashboard) and new CDM tool demonstrations.

The contractor shall provide an RDT&E environment that presents a realistic representation of the shared service platform operating environments. This will enable expanded end-to-end testing capabilities to ensure proper performance and functionality exists. The contractor shall use simulated CDM data that is representative of expected production data. This should include data that is similar in quantity and structure to that used or created by the tools and sensors that are commonly deployed at agencies supported by the Shared Services Platform.

The Government shall have access to the RDT&E environment. The contractor shall produce additional environments (e.g., training/test environment, demonstration sandbox) in coordination with the Government to support specific shared services platform stakeholders.

C.5.6 TASK 6 – INTEGRATE AGENCIES ON THE SHARED SERVICES PLATFORMS 1.0 AND 2.0:

This task includes onboarding all agencies supported by the current CDM Shared Services TO2F environment and any agencies not on the CDM Shared Services TO2F environment to the new DEFEND F Shared Services Platform and CDM Capabilities available through the SSC. Integration of agencies shall include the data from agency tools and sensors that support the CDM solution, as well as providing access to the CDM capabilities for users within the agency. The contractor shall manage each individual agency effort to ensure continuity of CDM functional support. It is the Government's intent for this task to mostly be performed for Shared Services Platform 2.0. However, the contractor shall integrate new agencies to the Shared Services Platform 1.0, if operational needs require it, and the contractor shall support the Shared Services Platform 1.0 under Section C.5.7 below.

C.5.6.1 SUBTASK 6.1 – CUTOVER WORK PLAN (CWP)

The contractor shall complete a CWP (**Section F, Deliverable 35**) that shall detail the methodology, timelines, and resources necessary to move TO2F supported Federal agencies and any new Agencies to the Shared Services Platform. The CWP shall be included in the PMP (Section C.5.1.4).

The Government will review and approve the CWP. The CWP is a living document, and the contractor shall update it for review and approval by the Government whenever changes are made.

The CWP shall include, but is not limited to, the following information:

a. Approach to documenting individual agency requirements, stakeholder communication,

and scheduling cutover.

b. Plan to execute a TRR (**Section F, Deliverable 30**) with User Acceptance Testing, OTRR (**Section F, Deliverable 20**), and ORR (**Section F, Deliverable 21**).
c. Technical and project management approach to migrating current TO2F supported Federal agencies, to ensure no gaps in CDM service and minimal risk to agency data and systems. The approach shall also provide consideration for the operation of the Agency Dashboard, Federal Dashboard reporting, and the security of agency data.
d. ATO approach and addressing specific agency security requirements.
e. Agency specific integration considerations, including agency specific System Development Life Cycle (SDLC) requirements and data interchange with legacy applications. This may also include providing the agency with Subject Matter Expert (SME) support to assist the agency with planning and cutover tasks including deployment of CDM capabilities.
f. Resource and budget requirements, including software, hardware, level of effort, labor category mix, Tools, ODCs, and Cloud resources.
g. The master schedule, including milestones of agency migrations to the new environment.
h. Cutover testing, agency sign-off, and governance.
i. Back-out plan and risk mitigation.
j. Technical and project management approach including WBS to add currently unsupported agencies to the Shared Services Platform.
k. Any Government or third party coordination requirements.
l. Training approach, including materials and any training environments to ensure agency staff is able to operate the implemented tools.
m. Data retention of existing data.
n. Overlap in Shared Service Platform functionality.
o. Transition to operations.

The COR, in coordination with the DHS TPOC, may require that new Federal agencies be added to the CWP. In this case, the contractor shall update the CWP to accommodate the additional agencies.

The contractor shall complete a TRR (**Section F, Deliverable 30**) following successful completion of the SRR. The Government will provide the contractor with direction to proceed with planned testing activities if the criteria have been met per the checklist provided in the CDM IV&V strategy.

C.5.6.2 SUBTASK 6.2 – AGENCY INTEGRATION CUTOVER

In accordance with the Government approved CWP, the contractor shall cut-over individual agencies from the TO2F environment, or add new Federal agencies to the Shared Services Platform 2.0. The contractor shall perform the work based on the master schedule in the CWP.

This may include providing the agency with SME support to assist the agency with planning and cutover tasks, including deployment of CDM capabilities.

In conjunction with the onboarding activities, the contractor shall concurrently complete three SELC Gate reviews and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**) for the following gates:

a. User Acceptance Testing TRR (**Section F, Deliverable 30**)
b. OTRR (**Section F, Deliverable 20**)
c. ORR (**Section F, Deliverable 21**)

Completion of these gates is possible only after the contractor has met all exit criteria as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**).

At completion of the work, testing, and validation for each agency, the contractor shall complete an Integration Report (**Section F, Deliverable 40**). The report shall contain, but not be limited to:

a. Documentation of cutover confirmation from the Government stakeholders at the agency, and the DHS TPOC.
b. Final levels of effort, and labor categories expended in the effort.
c. ODCs and Tools used in the effort.
d. Any open issues that must be tracked from an overall program perspective.
e. Lessons learned and a synopsis of any techniques, software code, or documentation that were added to the program knowledge base (Section 5.7.6).
f. Final milestone status; such as early, on-time and late.

C.5.6.3 SUBTASK 6.3 – IMPLEMENTATION OF ADDITIONAL SHARED SERVICES PLATFORM 2.0 SSC ITEMS FOR SUPPORTED AGENCIES

As new CDM capabilities are added to the SSC through upgrades to the Shared Services Platform 2.0, Supported Federal agencies may require that these CDM capabilities be implemented into their agency environments. In this case, the COR, in coordination with the DHS TPOC, will require the contractor to provide an estimate of tools, ODCs, hours by labor category, any Government-Furnished Property (GFP) needs, and timeline to implement the required capabilities or tools for the agency (**Section F, Deliverable 41**).

Upon approval of the estimate by the COR, the contractor shall implement the required additional SSC items for the supported agency. The contractor shall use the procedures detailed in the CWP to plan and conduct the work. This may include providing the agency with SME support to assist the agency with planning and cutover tasks, including deployment of CDM capabilities. The contractor shall also provide support to the agency to coordinate any ATO requirements. Upon completion of the work, the contractor shall provide an Integration Report, as outlined in Section C.5.6.2.

C.5.7 TASK 7 – OPERATE SHARED SERVICES PLATFORMS 1.0 AND 2.0

The contractor shall support day-to-day management of the Shared Services Platform 2.0 and the SSC. To ensure there is no gap in CDM services, the contractor shall operate the Shared Services Platform 1.0 during the period starting at the end of the period of performance for the TO2F TO, until all supported agencies have moved off of the Shared Services Platform 1.0 and are on the Shared Services Platform 2.0.

C.5.7.1 SUBTASK 7.1 – TRANSITION AND PERFORM OPERATIONS OF THE

SHARED SERVICES PLATFORM 1.0

The contractor shall transition and operate the current Shared Services Platform 1.0. This will allow continuity of CDM services to supported Federal agencies during integration with the new Shared Services Platform 2.0. The Government intends for this subtask to end when all agencies on the Shared Services Platform 1.0 have been transitioned to and are operational on the Shared Services Platform 2.0. The contractor shall complete a Shared Services Platform 1.0 Take Over Plan (**Section F, Deliverable 42**) in accordance with Section F that details the methodology, timelines, and resources necessary, for the contractor to complete transfer of operations. **The contractor's plan shall not move the Shared Services Platform 1.0 to a different hosting provider. The plan shall be based on the contractor not making any significant changes to the structure, ATO or operation of the Shared Services Platform 1.0.** The draft plan shall be included in the PMP (Section C.5.1.4). The Government will review and approve the Draft Shared Services Platform 1.0 Take Over Plan, and provide any comments or revisions for inclusion into the final Take Over Plan (**Section F, Deliverable 42**).

The contractor shall not make changes to the hardware and software technologies in use with the existing Shared Services Platform 1.0 solution and shall utilize existing service providers supporting the Shared Services Platform 1.0 solution. Existing service providers supporting the solution are: (1) *Govplace* for bundled service offering consisting of software and hardware to securely access the data center/cloud hosting operations environment, (2) *GDT* (formerly QTS (formerly Carpathia)) data center/cloud hosting provider for storage, memory and compute resources offered as a service through Govplace, and (3) *Palo Alto Networks* software subscription service for virtual firewall software to support the smallest Government agencies only (referred to as the OV4 agencies). The contractor shall adhere to all requirements to maintain the ATO by DHS for the Shared Services Platform 1.0 solution.

The Take Over Plan shall include, but is not limited to, the following information:

a. Project management approach, including WBS.
b. Stakeholder identification and communications.
c. Technical approach to transition, including management and identification of all data integration requirements.
d. ATO and security requirements.
e. Agency specific integration considerations, including data interchange with legacy applications.
f. A budget including software, hardware, level of effort by labor category, and cloud service provider related costs.
g. Project schedule, including milestones.
h. Testing, DHS sign-off, and governance.
i. Back-out plan and risk mitigation.
j. Any Government or third party coordination requirements, including GFP.

After Government approval of the Shared Services Platform 1.0 Take Over Plan, the contractor shall execute the hand over in accordance with the approved plan.

The contractor shall operate the Shared Services Platform 1.0 in accordance with the

requirements listed in subtasks (Sections C.5.7.2 – C.5.7.3) below.

C.5.7.2 SUBTASK 7.2 – OPERATE, MAINTAIN, AND PROVIDE SYSTEM ADMINISTRATIVE SERVICES FOR THE SHARED SERVICES PLATFORM

The contractor shall operate and maintain the Shared Services Platforms (1.0 and 2.0). The contractor shall operate Shared Services Platform 1.0 until all agencies have completed cutover to the Shared Services Platform 2.0, and are operational. The contractor shall also upgrade the platforms to accommodate any enhancements of existing capabilities and/or addition of new capabilities. The CDM Shared Services Platform environments' operational schedule shall be 24 hours a day, seven days a week (24x7).

The contractor shall install, configure, and integrate CDM capabilities and tools that support each new iterative addition to the SSC. As part of the implementation, the contractor shall implement the final version of software, as appropriate, in the cloud environment, including configuration, installation, integration, account migration services, and transition to follow-on operations in production. The contractor shall conduct quality assurance and integration testing for each release to verify acceptable interoperability between the Federal and agency dashboards and/or their capabilities.

The contractor shall develop a Plan for Production Operations (**Section F, Deliverable 44**)**.** The Plan for Production Operations shall describe how the contractor intends to operate the Shared Services Platform. The contractor shall perform O&M for the Shared Services Platforms in accordance with Plan for Production Operations once approved by the Government. The Plan for Production Operations shall include, but not be limited to:

a. Identification of requirements needed to operate the Shared Services Platforms (1.0 and 2.0).
b. Description of detailed O&M activities that are required for successful ongoing operations, including, at a minimum, the following:
    1. Identification of problems and approach to fixing.
    2. Ways to improve/maintain the performance of the system.
    3. Methodology for continuously monitoring capabilities to support implementation reviews in order to verify operational requirements are being met.
    4. Implementation of patches/HotFixes/updates for continued secure operation of the dashboard(s).
    5. Conduct scheduled and unscheduled maintenance.
    6. Identify and maintain configuration/releases (e.g., security/patch administration).
    7. Maintain information security (e.g., security vulnerability scanning and auditing logs for suspicious behavior).
    8. Maintain Event Management (e.g., authorized service interruptions).
    9. Account Maintenance including provisioning, disabling, and removing accounts.
    10. Methodology for measuring availability metrics (up/down).
    11. Verifying and Validating recovery processes (e.g., Backups, snapshots, and integrity thereof).
c. Approach to providing technical services for all CDM tool components, the Agency Dashboard, and the solution as a whole, whether from a single source or multiple sources.

d. Approach to operating the Shared Services Platforms consistent with the system security requirements of the hosting environment.
e. Description of the configuration management and change management methodology for CDM tools, including the hosting environment, in accordance with DHS policy.
f. Approach to monitoring and maintaining system capacity, and procedures for scaling cloud services to meet requirements.
g. Recommended operational service levels.
h. Tools and ODCs tracking including license management to the agency support level.
i. Operation of information exchange and data feeds from agencies and notification procedures when data channels are interrupted.
j. Planning, execution, and management of data backup, Disaster Recovery (DR), and Continuity of Operations (COOP) as directed by the DHS TPOC with the coordination of the COR.
k. Maintaining the ATO.
l. Any GFP requirements.
m. Approach to transitioning of agencies off the Shared Services Platform.

The contractor shall complete the Post Implementation Review (PIR) (**Section F, Deliverable 45**) SELC Gate and deliver all corresponding artifacts, as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**). The PIR shall be conducted approximately every six months with the intent to validate that the Shared Services Platform is operating correctly and providing value. Completion of the PIR gate review is only possible when the contractor has met all exit criteria as defined in the DEFEND F SELC Process Overview (**Section J, Attachment DD**).

C.5.7.3 SUBTASK 7.3 – PROVIDE THE SHARED SERVICES PLATFORMS HELP DESK AND TIERS I, II, AND III SERVICES

The contractor shall provide Help Desk and Tiers I, II, and III services for the Shared Services Platforms 1.0 and 2.0. The helpdesk shall not cover agency specific services, or those CDM services hosted at the agency level. The supported agencies will handle Tier I responsibilities for all functionality residing within the agency system boundary. For all operational service requests, the contractor shall establish a procedure for recording and a ticket tracking mechanism. The contractor shall provide services during a normal workweek (i.e., Monday through Friday) and provide coverage from 7:00 a.m. to 5:00 p.m. Eastern Time (ET) daily. In addition to normal working hours, the contractor shall be available during off hours (24x7) to remediate escalated issues.

The contractor shall provide a Help Desk capability for the cloud environment. Help Desk services shall include customer self-help services, online services and customer representative services supported by a “one number to call (e.g., hot-line) capability.” The “one number to call (e.g., hot-line capability)” shall serve as a central POC between the customer and the IT organization to resolve customer issues and provide a consistent and quality customer experience through the use of qualified staff, standardized processes, and an extensive knowledge management system. The Help Desk, supported by a common IT Service Management (ITSM) tool set, shall provide the ability to document, process, and monitor incidents, problems, inquiries, and change and service requests, as well as coordinate new capabilities through an

actionable service catalog and support for other ITSM functions. The contractor shall ensure that the Government has access to ITSM or other Help Desk support tools the contractor uses.

The contractor shall provide Tier I services for the CDM shared services environments, which shall include, but are not limited to, the following:

a. Problem resolution using standard methodologies.
b. Basic troubleshooting techniques.
c. Incident and request management.
d. Access and inventory management.
e. Change and configuration management.
f. Security and patch management consistent with the agreed to policies and procedures.

The contractor shall provide Tier II services for the CDM shared services cloud environments. Tier II support shall include, but is not limited to, in-depth troubleshooting with specialized knowledge of the Shared Services Platforms, or their sub-components/capabilities, for remediation.

The contractor shall provide Tier III services for the CDM shared services cloud environments. Tier III services shall include, but are not limited to, advanced engineering activities including coordination and resolution with solution Original Equipment Manufacturers (OEM).

On a monthly basis, the contractor shall report the ticket inflow, to include the total number of tickets received, types of issues, and how they were resolved (**Section F, Deliverable 46**). The contractor shall, at a minimum, provide the following services:

a. Provide initial problem resolution, where possible.
b. Generate, monitor, and track incidents through resolution, including metrics identifying time opened, time worked, time closed, and the parties' assigned responsibility through resolution.
c. Provide software support.
d. Maintain Frequently Asked Questions (FAQs) (**Section F, Deliverable 47**) and their resolutions.
e. Obtain customer feedback and conduct surveys.

C.5.7.4 SUBTASK 7.4 – MAINTAIN DATA QUALITY OF OPERATING SHARED SERVICES PLATFORM

The contractor shall ensure that the data collected, integrated, and reported within the Shared Services Platform, as evident in the Agency Dashboard and summarized at the Federal Dashboard, is of sufficient quality to ensure mission operational effectiveness. Specifically, the contractor shall ensure that the data from the underlying CDM supporting technologies has the following properties:

a. Complete: CDM asset coverage requirements must be adhered to and all required data elements must be presented, and integrated into the Agency Dashboard.
b. Current: Data must adhere to CDM data currency requirements (within 72 hours).

c. Accurate: Data must include all assets found in the agency, additionally data should be aged out as appropriate to ensure the most accurate representation of an agency's IT architecture (and its underlying assets) is reflected in the data.
d. Available: Results are accessible to the various CDM stakeholders.

The contractor shall proactively work to resolve any data inconsistency issues, including by working directly with Agencies to ensure timely resolution of any data issues.

C.5.7.5 SUBTASK 7.5 – DECOMMISSION SHARED SERVICES PLATFORM 1.0

Once all supported agencies are on the Shared Services Platform 2.0, the Government will direct the contractor to decommission the Shared Services Platform 1.0. Upon completion of the CWP , the contractor shall complete a Shared Services Platform 1.0 Decommission Plan (**Section F, Deliverable 48**). The COR and DHS TPOC will review the plan and provide any comments. The contractor shall finalize the plan based on Government comments (**Section F, Deliverable 49**), and perform the tasks outlined in the final plan. The Shared Services Platform 1.0 Decommission Plan shall contain, but is not limited to:

a. Disposition of any GFP and Government-Furnished Information (GFI).
b. ATO and data security considerations for any stored data.
c. Testing and coordination with any agency or external providers to ensure other systems are not affected by the decommission.

Upon Government direction, the contractor shall perform the tasks in the Final Decommission Plan.

C.5.7.6 SUBTASK 7.6 – PROVIDE KNOWLEDGE MANAGEMENT SERVICES

The contractor shall provide a centralized electronic Master Repository (**Section F, Deliverable 15**) that shall be accessible by Government stakeholders. The purpose of the repository is to maintain all Shared Services Platform documentation, program information, Travel Authorization Requests (TARs), Requests to Initiate Purchase (RIPs), deliverables, lessons learned, code, and techniques for agency implementations of the Shared Services Platform 2.0. The contractor shall provide the professional services necessary to operate and maintain the repository.

The Master Repository shall be developed and maintained in accordance with Section F. Along with copies of the documents the Master Repository shall include the following data for each document:

a. Dates submitted and approved by the Government
b. Financial information (i.e., estimated costs and costs invoiced) if applicable
c. Status of any pending Government actions
d. Any other pertinent information associated with the repository items identified above.

The Master Repository shall be continuously updated as requests/deliverables are submitted/responded to by the Government. The Master Repository shall be on-line and remotely accessible through standard web browser, and allow Government personnel to download or view all contents to provide Government situational awareness during the TO.

The Master Repository shall have access control features to allow access to documents and data

based on role. Supported agency Government stakeholders shall only have access to lessons learned, implementation code, and techniques for agency implementations. Only Government and contractor personnel associated with the performance of this TO shall be able to access the program information such as TARs, RIPs, and deliverables.

The contractor shall present a Master Repository inventory format at the Project Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the COR and this approved format shall be utilized throughout the TO period of performance. The Government may request updates to the format based on CDM Program Management Office (PMO) repository requirements. The contractor shall request any changes to the format in writing to the COR. The contractor shall deliver a database copy of the cumulative contents of the Master Repository every six months (**Section F, Deliverable 15**) and upon Government request.

C.5.7.7 SUBTASK 7.7 -- SOURCE, OBJECT, EXECUTABLE, AND RUN-TIME CODE

The contractor shall provide the most current version(s) and release(s) of any and all source, object, executable, and run-time code (as applicable) developed under the efforts of this TO ("New Code") and unique enhancements, customizations, and plug-ins, and other similar artifacts ("Customizations") to the Government (**Section F, Deliverable 50**) in accordance with the delivery requirements in **Section H.16.7**, Rights in New Code.

C.5.7.8 SUBTASK 7.8 – MAINTAIN AND MANAGE SOFTWARE INVENTORIES AND LICENSES

The contractor shall maintain an inventory of all software licenses used for the development and implementation of the Shared Services Platforms 1.0 and 2.0. The contractor shall manage software license renewals for this software, ensuring that all third party licenses are current. The contractor shall provide the Government a status of all third party licenses and inventories upon request from the CO or COR (**Section F, Deliverable 54**).

C.5.8 TASK 8 – STAKEHOLDER ENGAGEMENT

This task includes contractor support for stakeholder outreach, information, and training. The contractor shall support efforts to inform US Federal agencies about CDM Services, the Shared Services Platform 2.0, and the SSC. The contractor shall provide a thorough training program that ensures agencies are appropriately trained on all aspects of the DEFEND F solution.

C.5.8.1 SUBTASK 8.1 – PROVIDE CDM SOLUTION TRAINING

The contractor shall provide training on implementation and operation of an agency's CDM Solution on the Shared Services Platform 2.0, including the operation of individual CDM tools. Training shall ensure agencies can benefit from the dashboard information and sensor tool data, leading to improved effectiveness of the cyber posture at each agency.

The contractor shall deliver CDM Solution Training Plan Documentation (**Section F, Deliverable 51**) consisting of all training materials, any training manuals, COTS manuals for all installed CDM-related tools, and a Training Plan for each Group F Agency (**Section J, Attachment P**). At a minimum, the Training Plan shall include the following:

a. Training method.
b. Training medium.
c. Training tools.
d. Frequency of training.
e. Audience.
f. Location.
g. Method to incorporate training feedback.

The contractor shall ensure all training is consistent with the DHS-provided CDM Program training content and shall enable security and other agency staff to fully utilize the information provided by the CDM tools and dashboard. The DHS CDM training content provides an overview of CDM concepts, principles, and approaches for all capabilities of the CDM Program and how CDM capabilities work together.

At a minimum, the contractor shall deliver the following CDM Solution-based training:

a. **CDM Solution Effectiveness Training**. The contractor shall conduct this training prior to deploying new CDM capabilities in an agency's CDM environment. This training shall include detailed information on how the agency can operationalize CDM Dashboard metrics. Operationalize means to ensure the data provided is valued and used to improve the cyber posture of the agency. Such training ensures that the solution set provided by CDM is effective in strengthening the agency's cyber operations.
b. **CDM Solution Technical Training**. The contractor shall provide training on the CDM Solution product configuration, integration, and operations as they relate to an agency's network environment. This training is not intended to replace manufacturer's certification training. This training shall be role-based and consist of two subsets of training, specifically:
    1. CDM Tools-specific hands-on training for the user community, which allows the end-user to experience operations and the use of specific tools at the agency, and the tools located in the shared services platform, including vendor based product training. This training can be provided at a contractor facility, virtually, or at the agency site.
    2. Scenario-based training that exposes users to real-world use of the entire CDM Solution. This training can be provided at a contractor facility, virtually, or at the agency site.

C.5.8.2 SUBTASK 8.2 – PROVIDE PROGRAM OUTREACH AND INFORMATION

As directed by the COR and DHS TPOC, the contractor shall support stakeholder outreach events. These events shall inform supported agency stakeholders and members of industry of the status and planned progress for the DEFEND F program. These events will either be held virtually or in physical locations. The contractor shall provide coordination of logistics, venue, documentation, and notification of target audiences.

C.5.8.3 SUBTASK 8.3 – PROVIDE GOVERNANCE SUPPORT

Governance is a necessary component for ensuring effective integration of technology into an Agency's cybersecurity program. Agencies are responsible for managing and maintaining cybersecurity specific controls by linking technologies with effective policies and procedures in

order to comply with Office of Management and Budget (OMB) guidelines; often described as an Agency's Information Security Continuous Monitoring (ISCM) program.

The contractor shall assist each Agency in incorporating CDM capabilities into specific cybersecurity or ISCM programs so that the following outcomes are effectively planned, implemented, and documented:

a. Increased and/or more efficient risk-reduction (also described as defect reduction) at Agencies utilizing the most current CDM Agency Dashboard release and supporting technologies.
b. Improved definitions of, or criteria related to, Agency risk-thresholds relative to the CDM architecture and any extant Agency policies or plans related to ISCM.
c. Support strategic planning to help agencies incorporate CDM into existing ISCM and other cyber programs; addressing organizational change and operational aspects, communications to multiple stakeholders as appropriate.
d. Identification or improved definition of Agency specific "desired states" for use within the CDM architecture in general and current CDM Agency Dashboards and supporting tools in particular, so defect reduction is more effectively or efficiently realized, and Agency machine-level policies for future automated ongoing assessment of current, applicable NIST SP 800-53 controls are met.

C.5.9 TASK 9 (OPTIONAL) – PROVIDE SOC SERVICES TO THE SHARED SERVICES PLATFORM 2.0

The contractor shall provide SOC services to the Shared Services Platform 2.0. The SOC services shall be provided in accordance with DHS 4300A Attachment F, Incident Response. SOC services shall include, but are not limited to, the following:

a. 24x7 SOC Services monitoring for all connections.
b. 24x7 SOC Services incident notifications such as up/down status.
c. Distributed Denial of Service and Availability Monitoring.
d. Integration of Security Information Event Management (SIEM) or SIEM equivalent capabilities to monitor environment in "real time" for active threats.
e. Triaging events to determine if an incident has occurred.
f. Coordination functions with the National Cybersecurity and Communications Integration Center/U.S.-Computer Emergency Readiness Team, and/or other external Government security staff for incident management.
g. Notification of DHS and supported agencies of any detected incidents affecting the agencies' networks within 24 hours, even if these incidents do not affect the Shared Services Platform 2.0.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the COR at DHS and Agency locations in the Washington D.C. metropolitan area.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. If the deliverable is adequate, the Government may accept it or provide comments for incorporation.

All of the Government’s comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government’s satisfaction why such comments should not be incorporated.

If the Government finds that a deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable version, the contractor shall arrange a meeting with the COR.

E.4 DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government’s comments and/or change requests and to resubmit the deliverable.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO or COR will provide written notification of acceptance or rejection (**Section J, Attachment H**) of all deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated impact to the award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a 12-month base period followed by five, 12-month option periods.

Base Period:	TBD at award
First Option Period:	TBD at award
Second Option Period:	TBD at award
Third Option Period:	TBD at award
Fourth Option Period:	TBD at award
Fifth Option Period:	TBD at award

F.2 PLACE OF PERFORMANCE

The primary place of performance will be in the greater Washington, D.C. area with occasional travel within the Continental U.S. (CONUS) to support various stakeholder requirements. The primary place of performance will be at the contractor's site.

F.3 TO SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
NLT: No Later Than
PS: Project Start
TOA: Task Order Award
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14

RS: Restricted Software, per FAR 27.404-2 and 52.227-14

LD: Limited Rights Data, per FAR 27.404-2 and 52.227-14

SW: Special Works, per FAR 27.405-1 and 52.227-17

For software or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open source COTS software. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR Section H.13.1 and H.13.2. For

purposes of the foregoing, the terms “collateral agreement,” “Supplier Agreement,” and “Commercial Supplier Agreement” have the same meaning.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV’T RIGHTS
	Project Start (PS)			TBD at Award	N/A
01	Kick-Off Meeting Agenda	X001	C.5.1.1	At least three days prior to the Kick-Off Meeting	UR
02	Kick-Off Meeting Minutes Report	X001	C.5.1.1	Within five days of Kick-Off Meeting	UR
03	Kick-Off Meeting	X001	C.5.1.1	Within ten days of Project Start	N/A
04	QMP	X001	C.5.1.1, C.5.1.6	Draft: Due with PMP. Final: Due 10 days after receipt of Government comments. Updates as required by changes in program.	UR
05	Agency Onboarding Tracking	X001	C.5.1.1	At Kick-Off Meeting and with Monthly Status Report	UR
06	Monthly Status Report	X001	C.5.1.2	Monthly, 10th calendar day of the next month)	UR
07	Monthly Technical Status Meeting	X001	C.5.1.3	Monthly	N/A
08	Technical Status Meeting Minutes	X001	C.5.1.3	Five days after meeting	UR
09	Transition-In Plan	X001	C.5.1.1, C.5.2	Draft: Due at Kick-Off Meeting Final: Due 10 days after receipt of Government comments	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
10	Project Management Plan	X001	C.5.1.1, C.5.1.4	Draft: Due at Kick-Off Meeting Final: Due 10 days after receipt of Government comments Updates: As project changes occur, no less frequently than annually.	UR
11	Software Documentation	X001	H.16.2	As required	LD
12	Shared Services Platform Documentation	X001	H.16.4	As required	UR
13	Trip Report(s)	X001	C.5.1.5	Within 10 days following completion of each trip	UR
14	Meeting Reports	X001	C.5.1.7	As required	UR
15	Master Repository List	X001	C.5.1.1, C.5.7.6	Initial format Due at Kick-Off Meeting. Updates: As documents and deliverables are produced. Data copy of all repository content due every six months, or as requested	UR
16	Financial Reporting	X001	C.5.1.1, C.5.1.8	Monthly starting 20 days after PS	UR
17	Procurement Report	X001	C.5.1.9	Monthly starting 20 days after PS	UR
18	Quarterly IPR Agenda	X001	C.5.1.10	Ten days before IPR meeting.	N/A
19	Transition-Out Plan	X001	C.5.3	Within six months of PS. Updates: As project changes occur, no less frequently than annually.	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
20	OTRR	X001	C.5.5.1 C.5.6.1	As required	UR
21	ORR	X001	C.5.5.1 C.5.6.1	As required	UR
22	Solution Design Review	X001	C.5.4	As required	UR
23	Shared Services Platform Roadmap and Innovation Document	X001	C.5.4.1	Initial document due within 60 days of PS. Updates monthly, or as requested after that	UR
24	Reserved				
25	AoA	X001	C.5.4.2	Initial within 60 days of PS. Every six months after initial AoA is completed, or as directed by the Government	UR
26	Reserved				
27	SDR	X001	C.5.4.3	Within 60 days of PS and as required	UR
28	SRR	X001	C.5.5.1	As required	UR
29	Test Plans	X001	C.5.5.1	As required	UR
30	TRR	X001	C.5.5.1, C.5.6.1, C.5.6.2	As required	UR
31	PRR	X001	C.5.5.1	As required	UR
32	System Security Documentation	X001	C.5.5.2	As required	UR
33	Security Authorization Documentation	X001	C.5.5.2	As required.	UR
34	Update to Security Authorization Package	X001	C.5.5.2	As required	UR
35	CWP	X001	C.5.1.1, C.5.6.1	Draft: Due at Kick-Off meeting. Final: Due 10 days after receipt of Government comments. Updates as required by changes in program.	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
36	IPR Meeting Report	X001	C.5.1.10	Within 10 days after an IPR	UR
37	IMS	X001	C.5.1.11	Baseline IMS due within 20 days of PS. Updates made monthly after that showing progress against Baseline	UR
38	Reserved				
39	Reserved				
40	Integration Report	X001	C.5.6.2	As required	UR
41	Agency Estimate	X001	C.5.6.3	As required	UR
42	Shared Services Platform 1.0 Take Over Plan	X001	C.5.1.1, C.5.7.1	Draft: Due at the Kick. Final: Due 10 days after receipt of Government comments. Updates as required by changes in program.	UR
43	IPR	X001	C.5.1.10	First IPR due within 80 days of PS. Follow-on IPRs quarterly after that.	UR
44	Plan for Production Operations	X001	C.5.7.2	NLT than 60 calendar days after PS	UR
45	Post Implementation Review	X001	C.5.7.2	NLT than 60 calendar days after completion of hand-over	UR
46	Help Desk Report	X001	C.5.7.3	Monthly	UR
47	Update Frequently Asked Questions	X001	C.5.7.3	Monthly	UR
48	Initial Decommission Plan	X001	C.5.7.5	Initial due as required. Final due 10 days after receipt of Government comments	UR
49	Reserved				
50	Source Code	X001	C.5.7.7	As required	SW

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
51	CDM Solution Training Plan Documentation	X001	C.5.8.1	As required	UR
52	Redacted TO	X001	F.4	NLT than 10 days after TOA	UR
53	SCRM Plan	X001	H.5.1	NLT than 30 calendar days after PS	UR
54	Software License Inventory	X001	C.5.7.8	Upon request from CO or COR	UR

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (**Section F, Deliverable 52**). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S. Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in DHS' designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text Microsoft (MS) Word, PDF
b. Spreadsheets MS Excel

c. Briefings MS PowerPoint
d. Drawings MS Visio
e. Schedules MS Project

F.6 PLACE(S) OF DELIVERY

Copies of all deliverables shall be delivered to the COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Bob Hribar, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 501-1303
Email: robert.hribar@gsa.gov

Copies of all deliverables shall also be delivered to the DHS TPOC. The DHS TPOC name, address, and contact information will be provided at award.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR via a PNR (**Section J, Attachment E**) 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 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.

F.8 NEW SOFTWARE DELIVERY

Reference Section C.5.7.7, Source, Object, Executable, and Run-Time Code, if new software is required, in addition, the following applies:

Each software deliverable shall include the following: source, object, executable, and/or run-time code (as applicable), programmer notes, installation manual, user manual, administrator's manual, operations manual (or the like), other software documentation, including a detailed design description/explanation and a process for configuration management (i.e., everything that a programmer skilled in the art would need to maintain and upgrade the software with no additional instruction). The contractor shall specify which deliverable, or part thereof, is "New Code" versus "Customization," as defined in Section C.5.7.7. The contractor shall deliver each deliverable accompanied by evidence of assignment of copyright to the New Code and/or Customization portion of the deliverable (as applicable) in accordance with the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007).

The source, object, executable, and run-time code (as applicable), with their associated documentation and other materials as specified above, shall be delivered to DHS CDM Program Office on dates established in accordance with Section F.5, but in any event, NLT 30 calendar days before the termination/expiration of the TO. In the event the contractor defaults on the terms of this contract for any reason, the most current version of the source, object, executable, and run-time code shall be delivered to DHS CDM Program Office NLT 30 calendar days

following the event that leads to the termination/expiration of the TO, and the Government will retain the right to use any and all versions that are at that time installed at a Government facility, and to further develop and distribute them, with no royalties or other payments being due to the contractor or any other party.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The CO appointed a COR in writing through a COR Appointment Letter (Section J, Attachment A). The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Melanie Pollard
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: 202-969-7168 (C)
Email: melanie.pollard@gsa.gov

Contracting Officer's Representative:

Bob Hribar
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 501-1303
Email: robert.hribar@gsa.gov

Technical Point of Contact:

Provided at award.

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: 47QFCA20F0001

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*

FEDSIM Project Number: HS01007

Project Title: CDM DEFEND TO Group F

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned Identification (ID) and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the COR and DHS TPOC for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. Receipts shall be provided on an as-requested basis.

Each contract type shall be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. GWAC Number
b. TOA Number (NOT the Solicitation Number).
c. Contractor Invoice Number.
d. Contractor Name.
e. POC Information.
f. Current period of performance.
g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 CPAF CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Aliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
k. Any cost incurred not billed by CLIN (e.g., lagging costs).
l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Provide comments for deviation above 180 hours per month per employee.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP in **Section J, Attachment D** for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

G.3.2 TOOLS, AND ODCs COSTS

The contractor may invoice monthly on the basis of cost incurred for the Tools, and ODCs costs CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools, and ODCs purchased.

b. RIP or CTP number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.
h. Any applicable Fee

All cost presentations provided by the contractor shall also include any indirect costs being applied with associated cost center information.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulation (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the FTR/JTR. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.
g. Per diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding ten percent of the approved versus actual costs.
l. Indirect handling rate.

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.4 TO CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government will evaluate additional Key Personnel as proposed by the contractor.

All requirements of the TO apply equally to any proposed additional Key Personnel.

a. Project Manager (PM)
b. Lead Systems Integration Manager
c. Cyber Architect
d. Cyber Governance Lead

The Government desires that Key Personnel be assigned for the duration of the TO. Key Personnel may be replaced or removed subject to Section H.1.4, Key Personnel Substitution.

It is desirable for the contractor to achieve efficiencies in the composition of its proposed staffing. Although Key Personnel shall be available to support this TO at all times (assigned for the duration of the TO), full-time commitment by Key Personnel is not mandatory. Efficiencies may be achieved, for example, by sharing Key Personnel and/or non-Key Personnel across multiple agencies, and TOs.

H.1.1 PROJECT MANAGER (PM)

The contractor shall identify a PM to serve as the Government's main POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM shall ultimately be responsible for the quality and efficiency of the TO. The PM shall have organizational authority to execute the requirements of the TO. The PM shall assign tasking to contractor personnel, supervise ongoing technical efforts, and manage overall TO performance to ensure the optimal use of assigned resources and subcontractors. This Key Person shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. The PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual and programmatic issues.

It is required that the PM has the following qualifications:

a. Be an employee of the Prime contractor at the time of proposal submission.
b. Possess a Top Secret (TS) security clearance and have eligibility to access to Sensitive Compartmented Information (SCI) based on an SSBI, at the time of proposal submission.

It is desirable that the PM has the following qualifications:

a. Experience in completing, leading, or directing the work of others on projects similar to the size, scope, and complexity of the work and environment described in **Section C**.
b. Managerial experience providing technical advice, organizing, planning, directing, and managing staff to ensure goals and objectives are achieved.
c. Experience with the management and supervision of teams comprised of multi-disciplinary employees.

d. Experience with risk management, issue resolution, problem solving, and customer service.
e. Experience managing teams working on system architectures, networks, and operations.
f. Current Project Management Institute (PMI) Project Management Professional (PMP) or Program Management Professional (PgMP) certification.
g. A minimum of 15 years of experience managing complex, heterogeneous enterprise security integration projects across multiple disciplines for U.S. Government agencies.
h. A minimum of five years of experience as a Systems Engineer or Systems Architect, preferably for a U.S. Government Agency.
i. Possess three years or more of experience leading cloud based integration or development projects.

H.1.2 LEAD SYSTEMS INTEGRATION MANAGER

It is desirable that the Lead Systems Integration Manager has the following qualifications:

a. Current Certified Information Systems Security Professional (CISSP) certification.
b. A minimum of eight years of experience managing integration teams similar to the size, scope, and complexity of the work and environment described in **Section C**.
c. Experience implementing IT security projects in complex and heterogeneous environments, including the following:
    1. Experience developing, configuring, and delivering COTS software in support of enterprise security solutions.
    2. Experience leading integration planning activities of multiple U.S. Government agencies on a scale similar to this TO.
    3. Experience leading multi-organizational and matrixed technical resources and teams in accordance with approved integration plans and TO terms and conditions.
d. A minimum of six years of experience managing technical integration and solution delivery issues.
e. A minimum of four years of IT security operational experience, including assessment of information assurance and interoperability.
f. Demonstrated expertise in security policy and implementation.
g. Experience developing and integrating Continuous Monitoring capabilities.
h. A minimum of three years of experience deploying cyber-security solutions to cloud based platforms.
i. Possess a TS security clearance and be SCI eligible.

H.1.3 CYBER ARCHITECT

It is desirable that the Cyber Architect has the following qualifications:

a. Current CISSP certification.
b. A minimum of ten years of experience managing cyber architecture teams on projects similar to the size, scope, and complexity of the work and environment described in

Section C.

c. Experience developing cybersecurity solutions across a diverse and heterogeneous IT environment, including the following:
    1. Technical leadership in Enterprise Architecture (EA), Service Oriented Architecture (SOA), and IT Service Delivery to multiple U.S. Government agencies.
    2. Demonstrated experience in security solution design using existing and emerging technologies to achieve enterprise solutions.
d. A minimum of six years of experience working with Security Authorization requirements, developing and enhancing the security risk posture, and analyzing and reporting IT security metrics.
e. A minimum of four years of experience in security policy and emerging cybersecurity technologies.
f. A minimum of four years of experience deploying cyber-security applications to cloud based platforms.
g. Possess a TS security clearance and be SCI eligible.

H.1.4 CYBER GOVERNANCE LEAD

It is desirable that the Cyber Governance Lead has the following qualifications:

a. A minimum of eight years of experience providing demonstrably effective IT related governance support on projects similar to the size, scope, and complexity of the work and environment described in Section C, ensuring that customers realized positive benefits from new tools, policies, and procedures that were provided.
b. Experience developing and delivering effective cyber security policies and procedures to Federal agencies with ability to show positive results.
c. A minimum of six years of demonstrable experience working with IT stakeholders to develop and enhance cyber security risk postures by utilizing standardized and repeatable processes for IT risk identification and mitigation.
d. A minimum of four years of experience implementing effective IT governance programs to improve agency mission performance.
e. Possess a TS security clearance and be SCI eligible.

H.1.5 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to using other than personnel specified in proposals in response to a TO, the contractor shall notify the CO and the COR. This notification shall be NLT ten calendar days in advance of any proposed substitution and shall include justification (including Key Personnel Qualification Matrix (KPQM) for the proposed substitution, resume(s), and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the person being substituted. If the CO and the COR determine that a proposed substitute person is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of

the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost-Reimbursement).

H.1.6 PRIVACY STAFF QUALIFICATIONS

The target systems covered under the scope of this TO would not likely involve access to privacy information, including Sensitive Personally Identifiable Information (SPII). However, access may be required during the period of performance by changing operational requirements so the following terms apply:

The contractor shall designate privacy staff to support this TO.

The privacy staff shall be responsible for providing adequate support to DHS to ensure DHS can complete any required Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), or System of Records Notice (SORN) documents or other supporting documentation to support privacy compliance. The privacy staff shall work with personnel from the DHS CDM Program Office, the CISA Office of Privacy Office, the DHS Office of the Chief Information Officer (OCIO), the Records Management Branch, and any respective agency Privacy POCs to ensure that the privacy documentation are kept on schedule, answers to questions in the PIA are thorough and complete, and questions asked by the NPPD Office of Privacy and other offices are answered in a timely fashion.

See also Section H.4.5 Privacy Considerations.

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

As of the release of this TOR, the Government is not anticipating providing GFP. In the event the Government provides GFP, Section J, Attachment Y will be used for tracking purposes.

H.2.1 ACCOUNTABLE GOVERNMENT PROPERTY

As defined in FAR 52.245-1 (representing content as prescribed in FAR Part 45.107(a)(1)):

All contractor employees furnished with GFP shall ensure Government barcodes are not removed. In all GFP cases, the Government retains title to the property. It is the contractor's responsibility to use GFP as it was authorized, and for the purpose intended. In the event the contractor uses Government property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs. The contractor shall be directly responsible and accountable for all contract property in its possession in accordance with the requirements of the TO; this also includes any contract property in the possession or control of a subcontractor.

H.3 GOVERNMENT-FURNISHED INFORMATION (GFI)

Information about the agency IT/network environments and systems will be provided as GFI at TOA.

The contractor shall protect all GFI (e.g., Government data) by treating the information as Sensitive But Unclassified (SBU). SBU information and data shall only be disclosed to authorized-personnel as described in the TO herein. The contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information and data shall be returned to Government control, destroyed, or held until otherwise directed by the CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

If work under this TO requires that the contractor's personnel have access to Privacy Information, contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable agency rules and regulations.

H.4 SECURITY REQUIREMENTS

The Government requires all information pertaining to this TO be stored and protected in accordance with Government policy regarding SBU information. Therefore, no information shall be stored or transmitted outside the U.S. The information associated with this TO is critical infrastructure information as defined by 1016(e) of the U.S. Patriot Act of 2001 (42 U.S.C. 5195c(e)).

DHS security requirements are also applicable to this TO. In some instances, the contractor shall have to follow specific Agency security requirements that will be provided post-award as GFI.

H.4.1 PERSONNEL SECURITY CLEARANCES

At proposal submission only the contractor's PM shall possess a final TS security clearance, and be SCI-eligible. The Government will dictate the need for any additional security clearance requirements when applicable.

In general, all necessary employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.4.2 FACILITY CLEARANCE LEVEL (FCL)

At the time of proposal submittal, the contractor shall have a contractor facility with an approved facility clearance at the TS level. Although the TO utilizes information at the SBU level, the FCL will allow for greater classification levels as directed by the Government, should changes in requirements necessitate them.

An FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the Confidential, Secret, or TS level. The FCL includes the execution of a DoD Security Agreement (DD Form 441 and DD Form 441-1) and Certificate Pertaining to Foreign Interests (SF 328). Under the terms of a FCL agreement, the Government agrees to issue the FCL and inform the contractor as to the security classification of information to which the contractor will have access. The contractor, in turn, agrees to abide by the security requirements set forth in the National Industrial Security Program Operating Manual (NISPOM).

The Government will submit a DoD Contract Security Classification Specification (**Section J, Attachment V**) for the TS level post-award.

In general, all necessary FCLs shall be at the expense of the contractor.

H.4.3 DHS CONTRACTOR SECURITY REQUIREMENTS

H.4.3.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12)

The contractor shall provide a list of contractor personnel that require DHS badges and security clearances. The Government will process background investigations and/or security clearances for the contractor staff to occur after submission of the staff listing, provided the individuals meet the necessary security qualifications.

H.4.3.2 POST-AWARD SECURITY REQUIREMENTS

Contractors requiring access to DHS systems (including DHS GFP or CDM agency/Federal Dashboard) require personnel security vetting, including the scheduling and adjudication of the appropriate level of background investigation processed by the DHS Personnel Security Division (PSD). The DHS CDM PMO, in conjunction with the DHS PSD, shall have and exercise full control over granting, denying, withholding, or terminating unescorted Government facility and/or SBU Government information access for contractor employees, based upon the results of a background investigation. Contractor employees assigned to the TO not needing access to SBU agency information or recurring access to agency facilities shall not be subject to security suitability screening.

Contractor employees awaiting an Entry on Duty (EOD) decision may begin work on the TO provided they do not access SBU Government information. Limited access to Government buildings may be allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings, and begin transition work.

The contractor shall propose employees whose backgrounds offer the best prospect of obtaining a security badge approval for access. Non-U.S. citizens (foreign nationals or dual citizenships) are not permitted under this TO.

H.4.3.3 CONTRACTOR FITNESS DETERMINATION

The procedures outlined below shall be followed for the DHS Office of Security, PSD to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Contractor employees under the TO, requiring access to sensitive information, shall be able to obtain “DHS Suitability.” The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective contractor employees shall submit the following completed forms to the DHS Office of Security/PSD. The Standard Form (SF) 85P shall be completed electronically, through the OPM’s e-QIP System. The completed forms shall be given to the DHS Office of Security/PSD no more than three days after Project Start or 30 days prior to EOD of any employee, whether a replacement, addition, subcontractor employee, or vendor:

a. SF85P, “Questionnaire for Public Trust Positions”
b. FD Form 258, “Fingerprint Card” (two copies)
c. DHS Form 11000-6 “Conditional Access To Sensitive But Unclassified Information

Non-Disclosure Agreement"

d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of the TO.

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the Government do not relieve a contractor from performing under the terms of the TO.

DHS may, as it deems appropriate, authorize and grant a favorable EOD decision based on preliminary suitability checks. The favorable EOD decision would allow the employee to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information, at any time during the term of the TO. No employee of the contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five days of occurrence. The contractor shall return to the CDM Customer Representative (CR) all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the CDM CR, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel shall have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

DHS Security Office POC Information:

Office of Security/PSD
Customer Service Support
Washington, D.C. 20528
Telephone: (202) 447-5010

H.4.3.4 IT SECURITY TRAINING AND OVERSIGHT

All contractor employees accessing Government information systems, facilities, or data shall receive Security Awareness Training. This training will be provided by DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle SBU information within or under the supervision of the DHS shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS contractors with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems shall be continually monitored while performing these duties. The contractor's PM shall be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures shall be reported to the local Security Office or Information System Security Officer (ISSO).

Contractors who require access to Group F networks may also be required to complete Group F agency-specific security awareness training.

H.4.3.5 SBU NETWORK SECURITY REQUIREMENTS

Contractor employees (including applicants, temporaries, part-time, and replacement employees) under the TO, requiring access to SBU information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the TO. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective contractor employees shall submit the following completed forms to the DHS Security Office 30 days prior to EOD of any employee, whether a replacement, addition, or subcontractor employee:

a. SF85P, "Questionnaire for Public Trust Positions"
b. Form FD 258, "Fingerprint Card" (two copies)
b. DHS Form 11000-6, "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
c. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

DHS will provide the required forms at TOA. Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon TOA. Be advised that unless an applicant requiring access to SBU information has resided in the U.S. for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

H.4.3.6 INFORMATION ASSURANCE (IA)

This requirement implements the Government acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems to the extent that those requirements apply to the Group F Agencies and DHS. Contractor actions relating to information security must be in accordance with relevant Federal security statutes, regulations,

guidance, and memoranda. These statutes, regulations, guidance, and memoranda include, but are not limited to, the following:

a. FISMA of 2002
b. HSPD-12
c. Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.)
d. Public Law 106-398, Section 1061
e. OMB Circular A-130, *Management of Federal Information Resource*
f. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
g. OMB M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
h. OMB M-07-18 *Implementation of Commonly Accepted Security Configurations for Windows*
i. Operating Systems (Federal Desktop Core Configuration)
j. Federal Server Core Configuration Standard
k. NIST SP including the SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*
l. NIST SP including the SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*
m. NIST SP including the SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*
n. FIPS, including, but not be limited to, FIPS 140-2 *Security Requirements for Cryptographic Modules*, 199, and 200

These requirements safeguard IT services provided to agencies such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems. Along with these Federal requirements, any solution must comply with the standards detailed within the agency policies, which will be made available as needed. In addition to existing Federal standards and guidelines, it is the contractor's responsibility to adhere to new Federal standards/requirements that pertain to the security of unclassified information and information systems as these requirements are issued.

Information systems used or operated by the agency or by a contractor of the agency and DHS or other organization on behalf of the agency must be authorized to operate by the agency Authorizing Official (AO) through the Certification and Accreditation (C&A) process as outlined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The certification process verifies that information systems have employed security controls consistent with the sensitivity of the information maintained by the system as defined by FIPS 199 and SP 800-53 and acceptably meet Federal standards such as the list of regulations identified above. During the C&A process, the contractor is required to work with the Government in good faith and without question or delay to ensure that adequate mechanisms are in-place and used to protect information produced, processed, stored, and/or transmitted on or by the application.

The contractor shall provide all required documentation to support the agency's security authorization, including inputs to relevant portions of the Agency General Support System (GSS) SSP including descriptions of the management, operational, and technical security controls (as defined in NIST 800-53) employed in the system to the DHS TPOC and COR for agency approval. This security documentation shall be prepared consistent in form and content with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and include any additions/augmentations described in Agency IT Policy. The security documentation shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The documentation shall be reviewed and updated in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and FIPS 200 on an annual basis. Strict security requirements shall be imposed for work tasks that will be accomplished at the contractor facility including, but not limited to, the following:

a. Making configuration changes to improve security (harden the application) and/or otherwise address/mitigate discovered security vulnerabilities.
b. Providing all requested information and resolving any information security vulnerabilities identified by the Agency IA Office and/or detailed in the Security Test and Evaluation Report and/or Risk Assessment Report.
c. Documenting all system configurations in the Standard Install Process (SIP).

All activities performed at contractor facilities shall comply with the following:

a. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems.*
b. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*
c. NISPOM, DoD Manual, DoD 5220.22-M (when applicable).

The contractor shall not co-host agency systems with third-party sites that contain inappropriate content, which may include, but is not limited to, pornography, gambling, and political views.

The contractor shall not use agency equipment for activities that could be considered offensive or inappropriate, including activities that may:

a. Place undue burden on agency system components and resources.
b. Involve fundraising, non-agency commercial purposes, non- agency profit activities, stock trades, and gambling.
c. Result in access or transmission of objectionable material.
d. Incur additional cost to the agency.

In addition, webmail use on the agency equipment is strictly prohibited.

H.4.4 SECURITY SAFEGUARDS

The details of any safeguards the contractor may design or develop under this TO are the property of the Government and shall not be published or disclosed in any manner without the CO's express written consent.

The details of any safeguards that may be revealed to the contractor by the Government in the course of performance under the TO shall not be published or disclosed in any manner without the CO's express written consent.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the contractor shall afford the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases in accordance with FAR 52.239-1. The contractor shall use best efforts to ensure that the Government has similar access to the facilities, installations, technical capabilities, operations, documentation, records, and databases of its third-party hosting provider or sub-contractor.

If new or unanticipated IT security threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination of appropriateness being made by the Government.

H.4.5 PRIVACY CONSIDERATIONS

The target systems covered under the scope of this TO would not likely involve access to privacy information, including SPII. However, access may be required during the period of performance by changing operational requirements so the following terms apply:

H.4.5.1 REQUIRED SECURITY AND PRIVACY TRAINING

The contractor shall provide training for all employees and subcontractors that have access to SPII as well as the creation, use, dissemination, and/or destruction of SPII, at the outset of the subcontractor's/employee's work on the TO and every year thereafter. Training shall include procedures on how to properly handle SPII, to include security requirements for transporting or transmitting SPII information, requirements for reporting a suspected breach or loss of SPII within one hour, and supporting privacy compliance and breach management activities. The contractor shall submit an email notification to the COR and DHS TPOC that all the contractor's employees have received privacy training prior to the beginning of the TO.

The privacy training can be obtained via Government-provided compact disc (CD) or through the Homeland Security Information Network at https://share.dhs.gov/nppdprivacy101training/. DHS has also published a guidebook defining SPII and setting standards for SPII handling and protection. The DHS Handbook for Safeguarding SPII is a 30-page public document on the DHS Privacy Office website.

> http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

The Management Directive for "safeguarding of SBU information" and related policies require all individuals accessing NPPD information, regardless of their employment status, be they Federal or contractor employees, to take the Information Security and Records Management Training annually. Both courses (Information Security and Records Management) can be obtained via Government-provided CD. The contractor shall maintain copies of certificates as a record of compliance. The contractor shall submit an annual email notification to the COR and

DHS TPOC that the required Information Security, Records Management, and Privacy training has been completed for all the contractor's employees.

H.4.5.2 SUSPECTED LOSS OR COMPROMISE OF SPII (BREACH)

The contractor shall report the suspected loss or compromise of SPII by its employees or subcontractors to the DHS Help Desk at 1-800-250-7911 within one hour of the initial discovery.

The contractor shall also notify the CO, COR, and DHS TPOC via the Problem Notification Report (PNR) of the suspected loss or compromise. As part of the PNR, the contractor shall develop and include an Incident Response Plan, an internal system by which its employees and subcontractors are trained to identify and report potential loss or compromise of SPII. The PNR shall also include a written report within 24 hours of the suspected loss or compromise of SPII containing the following information (the written report shall also be provided to the NPPD Office of Privacy at NPPDPrivacy@hq.dhs.gov):

a. Narrative, detailed description of the events surrounding the suspected loss/compromise.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
e. Names of person(s) involved, including victim, contractor employee/subcontractor, and any witnesses.
f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

Notwithstanding any other remedies available to NPPD, the contractor shall indemnify the NPPD against all liability (including costs and fees) for any damages arising out of violations of this requirement.

The contractor shall cooperate with NPPD or other Government agency inquiries into the suspected loss or compromise of SPII to facilitate activities outlined in the DHS Privacy Incident Handling Guide (PIHG) and OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007. The DHS PIHG is an 88-page public document on the DHS Privacy Office website.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

At the Government's discretion, contractor employees or subcontractor employees may be identified as no longer eligible to access SPII or to work on the TO based on their actions related to the loss or compromise of SPII.

In the event that a SPII breach occurs as a result of the violation of a term of this TO by the contractor or its employees, the contractor shall, as directed by the CO and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing

notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor shall be responsible for reimbursing the Government for those expenses.

H.4.6 SECURITY COMPLIANCE REQUIREMENTS

H.4.6.1 COMPLIANCE WITH DHS SECURITY POLICY

All SBU systems employed by this TO must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A *Sensitive Systems Handbook*. All contractor systems used to process sensitive DHS data must be accredited for that use.

All national security systems produced by or supported under this TO must be compliant with DHS 4300B *DHS National Security System Policy*.

All DHS intelligence systems produced by or supported under this TO must be compliant with DHS 4300C *DHS Sensitive Compartmented Information (SCI) Systems Policy Directive*.

H.4.6.2 ACCESS TO UNCLASSIFIED FACILITIES, IT RESOURCES, AND SENSITIVE INFORMATION

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and TO performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. The contractor shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all TOs that require access to DHS facilities, IT resources, or sensitive information. The contractor shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the TO.

H.4.6.3 SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this TO are being implemented and enforced. The contractor shall afford DHS, including the organization of DHS Office of the CIO, the Office of the Inspector General, authorized CO, COR, and other Government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this TO. The contractor will contact the DHS CISO to coordinate and participate in the review and inspection activity of Government oversight organizations external to DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

H.4.6.4 SECURITY REQUIREMENTS FOR UNCLASSIFIED IT RESOURCES

All unclassified IT resources shall be managed and controlled in compliance with the DHS Acquisition Regulation (HSAR) clause 3004.470: Security requirements for access to unclassified facilities, IT resources, and sensitive information.

H.4.6.5 CONTRACTOR EMPLOYEE ACCESS

All contractor employee access shall be managed and controlled in compliance with HSAR clause 3004.470: Security requirements for access to unclassified facilities, IT resources, and sensitive information.

H.5 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

H.5.1 CONTRACTOR SAFEGUARDS

The contractor shall support supply chain protections as defined in the NIST 800-53 SA-12 control, which states, “The organization protects against supply chain threats to the information system, system component, or information system service by employing (Assignment: organization-defined security safeguards) as part of a comprehensive, defense-in-breadth information security strategy.” NIST 800-53 SA-12 can be located at the NIST website.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The contractor shall provide the Government with a SCRM Plan (**Section F, Deliverable 53)** that describes what safeguards it intends for supply chain protections which could include only using signed software.

H.5.2 COMPANY INFORMATION REVIEW

For the purposes of supply chain risk assessment under this TO, the “organization-defined security safeguards” referenced above will include a Government CO’s review of any negative findings reported by DHS as a result of the Company Information Review (CIR) conducted by DHS. The contractor is under a continuing obligation to ensure that all responses to the acquisition risk questions (**Section J, Attachment FF**) answered in the CIR remain complete, accurate, and up-to-date. The contractor shall promptly notify and submit updated responses to the CO when any change in circumstances of the contractor or subcontractors warrants a change in the contractor’s or subcontractor’s responses to the acquisition risk questions. In addition, the contractor is under a continuing obligation to promptly disclose to the CO any proposed additional or replacement subcontractors.

H.6 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.6.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

b. The contractor is required to complete and sign an OCI Statement (**Section J, Attachment K**). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

H.6.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) form (**Section J, Attachment L**) and ensure that all its personnel (including subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Execute and submit a Corporate NDA Form (**Section J, Attachment L**) prior to the commencement of any work on the TO.
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
c. Are instructed in Far Part 9 for third party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.7 IT ACCESSIBILITY FOR PERSONS WITH DISABILITIES

H.7.1 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's EIT Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor shall clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor shall ensure that the list is easily accessible by typical users beginning at time of award.

a. Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use Information and Communications Technology (ICT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All ICT that is procured, modified, developed, installed, configured, integrated, deployed, maintained and supported under this TOR shall comply with the applicable technical and functional performance criteria of the Section 508 standards unless a general exception applies.
b. When modifying commercially available or Government-owned ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance.
c. When providing and managing hosting services for ICT items, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance prior to providing the hosting service.
d. When providing installation, configuration, or integration services for ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
e. When providing maintenance upgrades, substitutions, and replacements to ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to upgrade, substitution or replacement.
f. When procuring ICT and where products that fully conform to the 508 Standards are not commercially available, the contractor shall procure the ICT that best meets the 508 Standards consistent with the agency's business needs (1194, 202.7 Best Meets). When applying this standard, all procurements of ICT shall have documentation of market research that identifies which provisions cannot be met by commercially available items, and the basis for determining that the ICT to be procured best meets the Standards consistent with meeting agency business needs as required by FAR 39.2. Any selection of a product or service that does not best meet the Revised 508 Standards due to a significant difficulty or expense shall only be permitted under an Undue Burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 139-05.

H.7.2 SECTION 508 ACCESSIBILITY STANDARDS

Revised 508 Standards: Applies to any component or portion of existing ICT purchased, developed, or altered under this TOR on or after January 18, 2018. Text of the standards and guidelines can be found at the United States Access Board website.

> https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines

Chapter 2: Scoping Requirements. Applies to all ICT procured, modified, developed, installed, configured, integrated, deployed, maintained and supported under this TOR.

Chapter 3: Functional Performance Criteria. Applies to all web and non-web based software procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this TOR that does not fully conform to Chapter 5: Software Technical Standards.

Chapter 4: Hardware Technical Standards. Applies to all hardware procured, modified, developed, installed, configured, integrated, deployed, maintained and supported under this TOR.

Chapter 5: Software Technical Standards. Applies to all web and non-web based software procured, modified, developed, installed, configured, integrated, deployed, maintained and supported under this TOR.

Chapter 6: Support Documentation & Services Technical Standards. Applies to all support documentation and services under this TOR.

Original 508 Standards: Applies to any components or portion of existing ICT that has not been altered on or after January 18, 2018 under this TOR, and fully complies with the Original 508 Standards.

Section 508 Conformance Testing Methods: DHS testing methods used to validate web and non-web electronic content for conformance to the Section 508 Standards.

a. Web and Software: https://www.dhs.gov/compliance-test-processes
b. Electronic reports and documentation in MS Office or Adobe PDF format https://www.dhs.gov/compliance-test-processes

H.7.3 SECTION 508 APPLICABLE EXCEPTIONS

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 139-05. DHS has identified the following exceptions that may apply: E202.4 Federal Contracts, all ICT that is exclusively owned and used by the contractor to fulfill this work statement does not require conformance with the Section 508 standards. This exception does not apply to any ICT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this TOR and for the purposes of this requirement, are not considered members of the public.

H.7.4 ACCEPTANCE CRITERIA

Prior to acceptance of ICT items that are developed, modified, or configured subject to this contract, the Government reserves the right to require the contractor to provide the following:

a. Accessibility test results based on the required test methods.
b. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
c. Documentation of core functions that cannot be accessed by persons with disabilities.
d. Documentation on how to configure and install the ICT Item to support accessibility.
e. Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

H.8 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract.

H.9 APPROVED PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the CO within ten workdays from the date the results are known to the contractor.

H.10 TRAVEL

H.10.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. JTR Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulation (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.10.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking long-distance travel to any Government site or any other site in performance of this TO, the contractor shall have this long-distance travel coordinated with the DHS TPOC and approved by the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (**Section J, Attachment M**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR or JTR.

Requests for long-distance travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Long-distance travel shall be scheduled during normal duty hours whenever possible.

H.11 TOOLS (HARDWARE/SOFTWARE), CLOUD COMPUTING SERVICES, AND/OR ODCs

The Government may require the contractor to purchase hardware, software, cloud services, and related supplies critical and related to the services being acquired under the TO. Such requirements will either be identified at the time a TOR is issued or may be identified during the course of the TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the COR and DHS TPOC a RIP (**Section J, Attachment N**). If the contractor is to lose an approved purchasing system at any time during TO performance (due to a temporary suspension of the Alliant 2 Prime contractor's purchasing system after TOA), the contractor shall submit to the CO a CTP (**Section J, Attachment O**) until such time that the purchasing system suspension has been lifted. The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. Where applicable, the GSA IT70 Schedule CDM Tool SIN cost should be used as one of the cost comparisons. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO and without complying with the requirements of Section H.13.

a. A Form DD1149 (**Section J, Attachment GG**) for each group of tools, as identified by manufacturer and/or receiving agency, that has been reviewed and signed by the receiving Agency to show concurrence.

b. A Form DD250 (**Section J, Attachment HH**) to match each Form DD1149 to be used upon delivery of tools as confirmation of receipt.

The contractor shall deliver the Form DD250s to the receiving agency along with the tools, cloud computing services or ODCs. The receiving agency POC will review the delivery for accuracy and show acceptance through signature on the DD250. The contractor shall email the signed DD250s to the COR for approval. Invoicing for procurements must have associated DD250s with the COR signature as supporting documentation.

H.11.1 TOOLS

Tools can be either specific to a CDM capability or ancillary. Tools that are specific to CDM capabilities (CDM tools) are identified on the CDM Approved Product List (APL). Information on the CDM APL can be found at http://www.gsa.gov/CDM.

If a tool specific to a CDM capability is identified as necessary to support the TO but is not on the APL, the contractor can request through the CDM APL Product Submission Instructions to add a tool. The DHS CDM PMO will make the determination for accepting the tool as part of the review and submission process.

H.12 EA COMPLIANCE TERMS AND CONDITIONS

All DHS-funded solutions and services shall meet DHS EA (referred to as Homeland Security (HLS) EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

a. All developed solutions and requirements shall be compliant with the HLS EA.
b. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
c. Description information for all data assets, information exchanges, and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and EA Information Repository.
d. Development of data assets, information exchanges, and data standards shall comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts shall be developed and validated according to DHS data management architectural guidelines.
e. Applicability of Internet Protocol Version 6 (IPv6) to Hosts, Routers, Systems (HRS)-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile NIST SP 500-267 and the corresponding declarations of conformance defined in the USGv6 Test Program.

H.13 COMMERCIAL SUPPLIER AGREEMENTS

H.13.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in **Section C** and as contemplated in the Tools and ODC CLINs in **Section B.4** may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). For purposes of this TO,

the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14.

H.13.2 The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state, and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor’s cloud; and (d) the creation of New Code and/or Customizations as contemplated in sections C.5.7.7 and H.16.7. The above rights constitute “other rights and limitations” as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

H.14 PRESS/NEWS RELEASE

The contractor shall not make any press/news releases pertaining to this procurement without prior Government approval and only in coordination with the CO.

H.15 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.16 SOFTWARE

H.16.1 SOFTWARE AGREEMENTS

All software used in the Shared Services Platform, including both COTS (e.g., GSA Schedule 70) and non-COTS (e.g., free open source, free proprietary, and GOTS software) shall comply with:

a. General Services Administration Acquisition Regulation (GSAR) 552.212-4 Contract Terms and Conditions—Commercial Items (FAR Deviation) (February 2018)
b. GSAR 552.232-39 Unenforceability of Unauthorized Obligations. (FAR Deviation) (February 2018)

See Section I.

H.16.2 SOFTWARE MAINTENANCE, TECHNICAL SUPPORT, AND DOCUMENTATION

The contractor shall provide maintenance and upgrades, technical support, and documentation for all proposed software (**Section F, Deliverable 11**). Documentation includes the installation manual, system administration manual, user manual, operations manual, and release notes or their equivalents.

H.16.3 DEVELOPMENTAL AND OPERATIONAL SOFTWARE TOOLS

The contractor may provide developmental software tools that, while not a part of the CDM Solution, are used to design, build, test, or maintain the Solution. Possible examples are tools used to gather and document requirements; compilers used to generate object code but not needed thereafter; project management tools; and so on. Operational tools, in contrast, are tools needed to operate the solution, such as production data base management systems, run-time libraries, and interpreters.

H.16.4 SHARED SERVICES PLATFORM SOFTWARE

The contractor shall provide documentation of software that the contractor uses to implement the Shared Services Platform to the extent necessary to complete assessment and authorization (A&A) of the platform specifically and the CDM Solution generally (**see Section F, Deliverable 12**). These include User Manual(s), Interface Manual(s), and Operations Manual(s), or their equivalents. Documentation, maintenance, upgrades, and technical support of the Shared Services Platform infrastructure are the contractor's own concern and need not be disclosed to the Government except as necessary to maintain system authorization or resolve problems, such as problems with compatibility with Agencies' infrastructure.

H.16.5 MIXED SOURCE SOFTWARE

Current generation software products and solutions may be composed of software components of mixed provenance, (e.g., COTS from multiple vendors and custom code). The contractor shall identify software components in the design documents (**see Section F, Deliverables 15, 28, 30 and 31**). The design documents (CONOPS and Solution Implementation Architecture –As-Built) shall clearly distinguish each component and its relationships to the other components in both a narrative and diagram(s).

H.16.6 LICENSE TRANSFERS

As and when so directed by the Government, the contractor shall transfer the license of any CDM software procured under this TO for use on the Shared Services Platform or another CDM Solution device to another Government or other contractor-owned compatible device or devices consistent with the limits of that license, (e.g., the number of cores).

H.16.7 RIGHTS IN NEW CODE

Notwithstanding anything to the contrary in this TO or in any applicable Supplier Agreement, the Government shall have Unlimited Rights in accordance with the FAR clause at 52.227-17, Rights in Data – Special Works (Dec. 2007), in any and all New Code and/or Customizations as defined in **Section C.5.7.7**. Delivery of such New Code and Customizations is hereby required, on dates specified by the Contracting Officer but in any event no later than the date of the TO expiration or termination for any reason and shall be accompanied by documentary evidence of assignment of copyright.

H.16.8 DEFERRED ORDERING OF TECHNICAL DATA OR COMPUTER SOFTWARE

In addition to technical data or computer software specified elsewhere in this Task Order to be delivered hereunder, the Government may, at any time during the performance of this TO, or within a period of three years after acceptance of all items (other than technical data or computer software) to be delivered under this TO or the termination of this TO, order any technical data or computer software generated in the performance of this TO or any subcontract hereunder. When the technical data or computer software is ordered, the contractor shall be compensated for converting the data or computer software into the prescribed form, for reproduction and delivery.

The obligation to deliver the technical data of a subcontractor and pertaining to an item obtained from the contractor shall expire three years after the date the contractor accepts the last delivery of that item from that subcontractor under this TO. The Government's rights to use said data or computer software shall be pursuant to the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007) and the clause listed in **Section H.16.9**, Technical Data and Computer Software Developed Exclusively at Private Expense, of this TO.

H.16.9 TECHNICAL DATA AND COMPUTER SOFTWARE DEVELOPED EXCLUSIVELY AT PRIVATE EXPENSE

(a) For the purposes of rights in data in the operation of this TO, the definitions, the treatment of unauthorized data markings, and the treatment of omitted markings shall be in accordance with paragraphs (a), (e), and (f), respectively, of the clause at FAR 52.227-14 in effect on the date of TOA. The portions of FAR 52.227-14 that are not specifically addressed herein shall not apply to such data.

(b) To the extent that the deliverables under this TO are authorized by the Statement of Work (SOW) to contain either technical data or computer software developed exclusively at private expense, those data shall be subject to the Government’s rights below for the specific category of data and shall be marked only in accordance with the following terms:

(1) Limited Rights Technical Data. This TO may identify and specify the delivery of limited rights data, or the CO may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the contractor shall affix the following “Limited Rights Notice” to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Limited Rights Notice

(a) These data are submitted with limited rights under Government Task Order No. _____ (and subcontract _____, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure:

(1) Use (except for manufacture) by support service contractors.

(2) Evaluation by non-Government evaluators.

(3) Use (except for manufacture) by other contractors participating in the Government's program of which the specific TO is a part.

(4) Emergency repair or overhaul work.

(5) Release to a foreign Government, or its instrumentalities, if required to serve the interests of the U.S. Government, for information or evaluation, or for emergency repair or overhaul work by the foreign Government.

(b) This Notice shall be marked on any reproduction of these data, in whole or in part.

(2) Restricted Computer Software.

(i) This TO may identify and specify the delivery of restricted computer software, or the CO may require by written request the delivery of restricted computer software that has been withheld or would otherwise be entitled to be withheld. If delivery of that computer software is required, the Contractor shall affix the following "Restricted Rights Notice" to the computer software and the Government will treat the computer software, subject to paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Restricted Rights Notice

(a) This computer software is submitted with restricted rights under Government Task Order No. _____ (and subcontract _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the Task Order.

(b) This computer software may be—

(1) Used or copied for use in or with the computer(s) for which it was acquired, including use at any Government installation to which such computer(s) may be transferred;

(2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

(3) Reproduced for safekeeping (archives) or backup purposes;

(4) Modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights;

(5) Disclosed to and reproduced for use by support service contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and

(6) Used or copied for use in or transferred to a replacement computer.

(c) Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice.

(d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the TO.

(e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

(End of notice)

(ii) Where it is impractical to include the Restricted Rights Notice on restricted computer software, the following short-form Notice may be used instead:

Restricted Rights Notice Short Form

Use, reproduction, or disclosure is subject to restrictions set forth in TO No. _____ (and subcontract, if appropriate) with _____ (name of Contractor and subcontractor).

(End of notice)

(iii) If restricted computer software is delivered with the copyright notice of 17 U.S.C. 401, it will be presumed to be licensed to the Government without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

(End of Clause)

H.17 AWARD FEE

See the AFDP in **Section J, Attachment D**.

H.18 ASSOCIATE CONTRACTOR AGREEMENT (ACA)

The contractor shall establish an ACA with the CDM Dashboard Provider that defines the roles and responsibilities for the agency CDM Dashboard provided by the CDM Dashboard Provider. This agreement shall include the cooperative co-maintenance of the CDM Dashboard solution. The Government may require the contractor to execute additional ACAs during the TOR period of performance.

H.19 EA COMPLIANCE TERMS AND CONDITIONS

Applicability of IPv6 to Agency's-related Components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the Agency's EA (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile NIST SP 500-267 and the corresponding declarations of conformance defined in the USGv6 Test Program.

I.1 TO CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-14	Display of Hotline Poster(s) https://forms.oig.hhs.gov/hotlineoperations/posteren.aspx	OCT 2015
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2018
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2019
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	OCT 2018
52.216-7	Allowable Cost and Payment Fill in: 30 days	AUG 2018
52.219-8	Utilization of Small Business Concerns	OCT 2018
52.222-2	Payment for Overtime Premiums Fill-in: To be completed at TOA	JUL 1990
52.222-26	Equal Opportunity	SEP 2016
52.222-50	Combating Trafficking in Persons	JAN 2019
52.223-17	Affirmative Procurement of EPA Designated Items in Service and Construction Contracts	AUG 2018
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data –Alternate I	DEC 2007
52.227-14	Rights In Data –Alternate II	DEC 2007

FAR	TITLE	DATE
52.227-14	Rights in Data – Alternate III	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.227-21	Technical Data Declaration, Revision, and Withholding of Payment – Major Systems	MAY 2014
52.232-33	Payment by Electronic Funds Transfer – System for Award Management	OCT 2018
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.242-15	Stop-Work Order, Alternate I	APR 1984
52.244-6	Subcontracts for Commercial Items	JAN 2019
52.245-1	Government Property	JAN 2017
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-11	Higher Level Contract Quality Requirement	DEC 2014
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.217-7 OPTION TO INCREASE QUANTITY – SEPARATELY PRICED LINE ITEM (MAR 1989)

The Government may require the numbered line items, identified in the task order as Optional Contract Line Item Numbers (CLINs), in the quantity and at the price stated in the task order. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days. The Optional CLINs shall continue at the same rate specified in the task order, unless the parties otherwise agree.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days before the contract expires.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days before the contract expires; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the

contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 72 months.

(End of clause)

I.3 GSAM CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.215-70	Examination of Records by GSA	JUL 2016
552.232-25	Prompt Payment	NOV 2009
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018

I.4 DHS ACQUISITION REGULATION SUPPLEMENTS (HSAR) CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

HSAR	TITLE	DATE
HSAR Class Deviation 15-01	Safeguarding of Sensitive Information	MAR 2015

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TOR.

ATTACHMENT	TITLE
A	COR Appointment Letter
B	Reserved
C	Incremental Funding Chart (electronically attached .xls) (Attached at TOA)
D	Draft Award Fee Determination Plan (AFDP)
E	Problem Notification Report (PNR) Template
F	Monthly Status Report (MSR) Template
G	Trip Report Template
H	Deliverable Acceptance-Rejection Report Template
I	Corporate Experience Template (to be removed at time of award)
J	CDM Technical Capabilities Volume Two Requirements Catalog
K	Organizational Conflict of Interest (OCI) Statement
L	Corporate Non-Disclosure Agreement (NDA)
M	Travel Authorization Request (TAR) Template (electronically attached .xls)
N	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
O	Consent to Purchase (CTP) Template (electronically attached .xls)
P	CDM Training Events
Q	Cost/Price Excel Workbook (To be removed at time of award)
R	Project Staffing Plan Template (To be removed at time of award)
S	Key Personnel Qualification Matrix (KPQM) (To be removed at time of award)
T	Procurement Report Template
U	Electronic Reading Room Instructions
V	Contract Security Classification Specification
W	Offeror Q&A Template (To be removed at time of award)
X	Letter of Commitment Template (To be removed at time of award)
Y	GFP Tracking Template (Attached at TOA)
Z	Reserved
AA	Supported Agency List
BB	DEFEND F Initial SSC
CC	Shared Services Design Guidance and Conceptual Architecture
DD	DEFEND F SELC Process Overview
EE	Program Test and Evaluation Master Plan (TEMP) (Attached at TOA)
FF	Acquisition Risk Questions

ATTACHMENT	TITLE
GG	DD1149
HH	DD250
II	52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2019)

K.1 FEDERAL ACQUISITION REGULATION (FAR) PROVISIONS INCORPORATED BY FULL TEXT

See **Section J, Attachment II**

L.1 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

https://www.acquisition.gov/far

https://www.acquisition.gov/gsam/gsam.html/

FAR	TITLE	DATE
52.215-1	Instructions to Offerors-Competitive Acquisition	JAN 2017
52.215-22	Limitations on Pass-Through Charges – Identification of Subcontract Effort	OCT 2009
52.217-5	Evaluation of Options	JUL 1990
52.225-25	Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran – Representations and Certifications	AUG 2018
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.232-38	Submission of Electronic Funds Transfer Information with Offer	JUL 2013
52.237-10	Identification of Uncompensated Overtime	MAR 2015

L.1.1 SOLICITATION PROVISIONS PROVIDED IN FULL TEXT

FAR 52.215-20 Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data – Alternate IV (OCT 2010)

(a) Submission of certified cost or pricing data is not required.

(b) Provide data described below:

All data required to be submitted as part of the offeror's proposal is described in Sections L.5, L.6, and L.7 of this solicitation. The offeror must use the formats for submission of data prescribed in these sections. By submitting a proposal, the offeror grants the CO or an authorized representative the right to examine records that formed the basis for the pricing proposal. That examination can take place at any time before award. It may include those books, records, documents, and other types of factual data (regardless of form or whether the data are specifically referenced or included in the proposal as the basis for pricing) that will permit an adequate evaluation of the proposed price.

(End of provision)

L.2 GENERAL INSTRUCTIONS

a. The offeror is expected to examine this entire solicitation document including the Master/Basic Contract. Failure to do so will be at the offeror's own risk.

b. The Government may make award based on initial offers received, without discussion of such offers. Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments listed in Section J). The penalty for making false statements in proposals is prescribed in 18 U.S.C. 1001.

c. An offeror submitting restricted data shall mark it as follows in accordance with FAR 52.215-1, Instructions to Offerors - Competitive Acquisition, which is incorporated by reference. FAR Clause 52.215-1(e) states: "Restriction on disclosure and use of data. Offerors that include in their proposals data that they do not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes, shall –

(1) Mark the title page with the following legend:

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed--in whole or in part--for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of--or in connection with--the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]; and

(2) Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal."

d. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552).

e. This procurement is conducted under the procedures of FAR Subpart 16.5. The policies and procedures of FAR Subpart 15.3 do not apply.

L.3 GENERAL INFORMATION

The total estimated CPAF of the TO is between $144,500,000 and $160,600,000. The estimate does not include Tools, and ODCs costs, Long-Distance Travel, and CAF. Any proposal that is not within this range shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the offeror would like the Government to consider as the justification for the deviation from the range.

Proposals shall be valid for a period of not less than 120 calendar days from the date of delivery. **For proposal purposes only**, offerors shall use a Project Start date of **March, 31st, 2020.**

L.3.1 AVAILABILITY OF EQUIPMENT AND SOFTWARE

All commercial hardware and software proposed in response to this solicitation document shall have been formally announced for general release on or before the closing date of the solicitation. Failure to have equipment or software announced prior to submission of proposal may render the offeror's proposal NOT ACCEPTABLE.

All commercial and non-commercial hardware and software proposed in response to this solicitation document shall ***not*** have been formally announced as at its end of life or end of technical support by its publisher or licensor. Proposal of commercial or non-commercial hardware and software that is at its end of life may render the offeror's proposal NOT ACCEPTABLE.

L.3.2 CONTRACTOR SUPPORT DURING TECHNICAL EVALUATION

The Government expects to have contractor support during the evaluation from E3 Federal Solutions, LLC/Sentinel (E3/Sentinel). The prime offeror is encouraged to sign a Non-Disclosure Agreement (NDA) with E3/Sentinel for its submission. NDAs submitted by a prime offeror will be considered as including any subcontractors in the offeror's proposal; subcontractors should not submit separate NDAs (i.e., there should be only one NDA per team).

An offeror that chooses to enter into an NDA with E3/Sentinel shall coordinate with and submit its corporate NDA to the POC listed below, specifically referencing this solicitation's number and title in the NDA's scope. If an NDA is signed, the NDA shall be submitted with the proposal Part I submission. E3/Sentinel is prohibited from proposing on any work related to CDM DEFEND F TO. This instruction is not evaluated under Section M.

E3/Sentinel
POC: Thomas Eckl, Project Manager
Address: 8281 Greensboro Dr. #400, McLean, VA 22102
Telephone: 682-365-8409
Email: teckl@e3federal.com

L.4 SUBMISSION OF OFFERS

Each offer shall be provided to the Government in four parts. Parts I through III are separately bound. The submission shall contain the following:

a. Part I – Preliminary Written Cost/Price Proposal Information
b. Part II – Remainder of Written Cost/Price Proposal
c. Part III – Written Technical Proposal
d. Part IV – Video Technical Proposal Presentation

The offeror shall submit each Part on the due dates indicated on the Cover Letter.

Unless otherwise specified, one page is one side of a U.S. Letter size (8.5" x 11") piece of paper. All electronic files shall be in MS Word, PowerPoint, PDF, or Excel formats. Any documents provided in Section J, List of Attachments, shall be submitted using the same file format (e.g., Project Staffing Plan shall be submitted in Excel file format using the Excel template provided); this includes the same font size and margins as the document provided. Printed pages (with the exception of Excel and PowerPoint) must maintain one inch margins. Excel files must maintain

margins of no less than 0.7 inches, and PowerPoint files must maintain margins of no less than 0.5 inches. Printed pages must maintain 12 point Times New Roman font and be single spaced, with the exception of charts/graphics/tables. Charts/Graphics/Tables must maintain a minimum of ten point Times New Roman font, including in the Part IV slides. Charts/Graphics/Tables embedded in the proposal will count toward page limitations. Headers and footers may be of a font larger than 12 point, but shall not be smaller than ten point font. Ledger size (11" x 17") paper may be used in the Project Staffing Plan. A single side of an 11" x 17" piece of paper will be counted as two pages where page limitations apply. Items such as a Title Page, Table of Contents, Cover Letter, List of Figures, and Acronym Lists are excluded from the page counts below, unless they are inclusive of a document (e.g., a Table of Contents within the Transition-In Plan), in which case it would count toward the stated page limitations. PDF files will be allowed for executed documents such as Letters of Commitment.

Any pages submitted beyond the page limitations will be removed and not evaluated.

L.5 SUBMISSION OF THE WRITTEN COST/PRICE PROPOSAL (PARTS I and II)

Audits may be performed by DCAA on the offeror and all subcontracts. Cost/Price Proposals shall meet the DCAA audit submittal requirements. The offeror shall fully support all proposed costs/prices. An offeror's proposal is presumed to represent the offeror's best efforts in response to the solicitation. Any inconsistency, whether real or apparent, between promised performance and cost/price, shall be explained in the proposal.

The offeror shall provide adequate information, which will allow the Government to perform a Cost Realism analysis. Pursuant to FAR 15.404-1(d)(1), Cost Realism analysis is defined as:

> "…the process of independently reviewing and evaluating specific elements of each offeror's proposed cost estimate to determine whether the estimated proposed cost elements are realistic for the work to be performed; reflect a clear understanding of the requirements; and are consistent with the unique methods of performance and materials described in the offeror's technical proposal."

As indicated in Section L.1.1 under FAR Clause 52.215-20, a description of the data required to be submitted with the offeror's proposal in order to facilitate the Cost Realism analysis is provided below in Section L.5.2.4.

Written Cost/Price Proposals shall be submitted as one original printed version and one electronic copy. No thumb drives will be accepted. The offeror shall submit all proposed costs/prices using MS Excel software utilizing the formats without cells locked and including all formulas. The offeror shall include adequate information, which will allow the Government to perform the required Cost Realism analysis.

The offeror shall not include any cost/price data in Parts III and IV of the proposal.

L.5.1 PRELIMINARY WRITTEN COST/PRICE PROPOSAL INFORMATION (PART I)

Part I contains the Preliminary Written Cost/Price Proposal information. The offeror shall provide a Cover Letter that identifies a POC, DUNS number, Commercial and Government Entity (CAGE) code, and GWAC number. This volume shall contain the following:

a. Contract Registration (Tab A)

b. Current Forward Pricing Rate Agreements or Recommendations (Tab B)
c. Management Systems (Adequate Cost Accounting, Approved Purchasing Systems, and any other systems as applicable to this requirement) (Tab C)
d. Cost Accounting Standards (CAS) Disclosure Statement (D/S) (Tab D)
e. Reserved (Tab E)

L.5.1.1 CONTRACT REGISTRATION (TAB A)

The offeror shall submit a statement that the contract vehicle under which this proposal is being submitted has been registered in ASSIST and that all information in ASSIST is up-to-date. ASSIST can be accessed by visiting the following webpage:

https://portal.fas.gsa.gov/assist-web/registration/contractor/search

L.5.1.2 CURRENT FORWARD PRICING RATE AGREEMENTS OR RECOMMENDATIONS (TAB B)

The offeror shall submit all forward pricing rate agreements or recommendations including that of the prime contractor, any cost-type subcontractors, and/or proposed Joint Venture. Subcontractors may submit proprietary data directly to the CO or through the prime contractor in a separate sealed envelope.

If the offeror proposes any cost-type subcontracts with small businesses that do not have forward pricing rate agreements or recommendations, the offeror shall provide in its submission or via sealed envelope the following information for each applicable small business cost-type subcontractor:

a. Historical information for each indirect cost rate pool and the applicable base for the past five years and projections for the next five years.
b. A cost narrative that describes the corporate approach to cost accounting, how indirect costs are applied to direct costs, and a description of its accounting system's ability to segregate costs appropriately.

L.5.1.3 MANAGEMENT SYSTEMS (ADEQUATE COST ACCOUNTING AND APPROVED PURCHASING SYSTEM) (TAB C)

a. The offeror shall describe all applicable management systems (i.e., accounting, estimating, purchasing).
b. The offeror shall specifically include the date of the last DCAA/DCMA (or other cognizant Federal agency, if small business) cost accounting system and purchasing system audits, a copy of the results of the audits, audit report number, and date determined adequate. This shall include verification in a form acceptable to the Government of the currently determined adequate systems (e.g., copy of most recent Government purchasing system approval and Government Cost Accounting System adequacy letter).
c. The offeror shall include the name, office, and phone number of its cognizant DCAA/Government audit agency and DCMA/Government Administrative Contracting Officers (ACO) who are responsible for any cost accounting and purchasing system reviews of the contractor.

L.5.1.4 COST ACCOUNTING STANDARDS (CAS) DISCLOSURE STATEMENT (D/S) (TAB D)

The offeror shall include a copy of the CAS D/S. Also, the offer shall state the adequacy of D/S, date audited, audit report number, date determined adequate by ACO, and include any non-compliances with CAS.

L.5.1.5 RESERVED (TAB E)

L.5.2 REMAINDER OF WRITTEN COST/PRICE PROPOSAL (PART II)

Part II is the Remainder of Written Cost/Price Proposal and shall contain the following:

a. OCI Statement and NDA (Tab F)
b. Solicitation, Offer and Award (SF33) (Tab G)
c. Section B – Supplies or Services and Prices/Costs (Tab H). Do not include cost/price for six-month extension period authorized by FAR clause 52.217-8.
d. Cost/Price Supporting Documentation (Tab I)
e. Subcontractor Supporting Documentation (Tab J)
f. Cost/Price Assumptions (Tab K)
g. Representation of Limited Rights Data and Restricted Computer Software (Tab L)
h. Pass/Fail Elements (Tab M)
i. Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Tab N)

L.5.2.1 OCI STATEMENT AND NDA (TAB F)

The offeror and each subcontractor, consultant, and teaming partner involved in proposal development shall complete and sign an OCI Statement. All information pertaining to OCI is outlined in Section H.6.1.

If an offeror enters into an NDA with E3/Sentinel, the offeror may include the signed agreement in Tab F.

L.5.2.2 SOLICITATION, OFFER AND AWARD (SF 33) (TAB G)

When completed and signed by the offeror, Standard Form (SF) 33, “Solicitation, Offer and Award,” constitutes the offeror’s acceptance of the terms and conditions of the proposed TO. Therefore, the form must be executed by representatives of the offeror authorized to commit the offeror to contractual obligations. The offeror shall sign the SF 33 in Block 17.

The authorized negotiator or the signatory of the SF 33 will be notified of the date and time of the Oral Question and Answer Session. The offeror shall provide the name of the individual, the position title, telephone number, fax number, and email address of that individual.

L.5.2.3 SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS (TAB H)

The offeror shall indicate the cost/price to be charged for each item in **Section B** rounded to the nearest whole dollar. The offeror shall insert NTE indirect/material handling ceiling rates in accordance with Section B.5.1.

As a supplement to the summary information provided in Section B, the offeror shall provide full back-up documentation for the Labor CLINs for each period of performance and each task using the provided Cost/Price Excel Workbook (Section J, Attachment Q). The offeror shall complete all worksheets in the Cost/Price Excel Workbook in accordance with the instructions provided in the Cost/Price Excel Workbook. **The offeror shall not lock any cells and the offeror shall ensure all calculation formulas are included in order to effectively show the cost build up in the Cost/Price Excel Workbook.** The back-up documentation shall include a summary total for each element of cost (e.g., direct labor, OH, G&A, Facilities Capital Cost of Money (FCCM), fee, etc.).

L.5.2.4 COST/PRICE SUPPORTING DOCUMENTATION (TAB I)

The cost/price supporting documentation is required to enable the Government to perform cost or price analysis. The offeror shall provide the following cost/price supporting documentation:

a. Cost Narrative:
    1. The offeror shall provide a detailed cost narrative, which explains the processes and methodologies used to develop its cost/price proposal. This includes, but is not limited to, the estimating methodology used by the offeror to estimate direct labor and subcontractor labor, explanation of the application of indirect rates, planning assumptions used in the development of the cost estimate, etc.
    2. The offeror shall also include a crosswalk of its labor categories, basis of cost element, weightings, and explanations to those in the solicitation.
    3. The offeror shall specifically indicate in its narrative any applicable Uncompensated Overtime Policy and how such policy affects the hourly direct labor rates and Full-Time Equivalent (FTE) hours being proposed during any TO year.
b. Indirect Rate Information:
    1. The offeror shall break out all proposed indirect rates (OH, Fringe, G&A, etc.) by CLIN, by each applicable TO period, and by task.
    2. The offeror shall clearly identify the cost base from which each proposed indirect rate is being applied.
    3. Historical indirect rates (unburdened) shall be provided (OH, Fringe, G&A, etc.) for the last five years inclusive of appropriate explanations for any major increases and decreases in the rates between years.
c. Direct Labor Rate Information:
    1. The offeror shall provide the base direct labor rate (unburdened) for all proposed labor categories (Key and non-Key) and all projected rates (factoring in escalation) for all option years. The Key Personnel labor rates shall be supported by evidence of actual rates currently being paid and/or the basis for specific rates being proposed.
    2. The offeror shall identify all direct labor escalation factors and basis for any escalation index being utilized for all option years.
d. Fee Review:
    1. The offeror shall break out all proposed fees and clearly delineate the cost base in which the fee percentages are applied.

L.5.2.5 SUBCONTRACTOR SUPPORTING DOCUMENTATION (TAB J)

The offeror shall also provide supporting cost/price documentation for all proposed subcontractors, to include the total value of the proposed subcontract, the proposed type of subcontract, the rationale, and/or justification for this type of subcontract type, and how fee will be determined and paid. Additionally, the offeror shall provide a narrative detailing the processes used to evaluate the subcontracts it is proposing, including cost and/or price analysis conducted as appropriate for each subcontract. In addition to the supporting cost back-up documentation, DCAA contact information and relevant cost/pricing data shall be provided for all cost-type subcontractors. Failure to provide complete supporting documentation may result in no further consideration of the offeror's proposal. Subcontractors may submit proprietary data directly to the CO or through the prime contractor in a separate, sealed envelope. **The prime contractor shall specifically state whether the estimated costs of any proposed subcontractor will be in excess of $10M over the life of the TO for Government accomplished Equal Employment Opportunity (EEO) verification purposes.**

The prime offeror is responsible for ensuring that all cost-type subcontractors include the same type of cost detail in the same format as required in Section L.5.2.4. All non-cost subcontractors shall provide the following information:

a. Firm-Fixed-Price (FFP): A basis of estimate for the FFP amount is required which includes the LOE and fully burdened labor rates associated with the FFP amount.
b. Time and Materials (T&M)/Labor Hour (LH): The labor rate, the LOE, and supporting documentation to substantiate the proposed labor rates are required for the T&M amount. Supporting documentation could include past invoices, GSA schedule price lists, or other applicable information.
c. All proposed Alliant 2 labor categories should be mapped to the appropriate labor category in the supporting documentation, and a description of the labor categories should be provided.
d. If the proposed subcontractor does not possess an established acquisition vehicle (e.g., GSA Schedule), the subcontractor shall provide payroll/invoices or Commercial Catalogs for labor rate verification.

L.5.2.6 COST/PRICE ASSUMPTIONS (TAB K)

The offeror must submit all (if any) assumptions upon which the Cost/Price Proposal is based.

L.5.2.7 REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE (TAB L)

The offeror shall complete and provide the remainder of FAR 52.227-15(b), Representation of Limited Rights Data and Restricted Computer Software.

L.5.2.8 PASS/FAIL ELEMENTS (TAB M)

A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the Technical and Cost/Price proposal accomplished by the Government. The offeror shall provide:

a. Named Key Personnel: Each proposed Key Person shall be named at the time of proposal Part II submission. The offeror shall provide a list of Key Personnel, including position title and name (Section H.1, Key Personnel, and additional Key Personnel positions, if any). This list shall be consistent with the information provided in the **Section J, Attachment R**, Project Staffing Plan Template and **Section J, Attachment S**, Key Personnel Qualification Matrix (KPQM) in the Written Technical Proposal. A proposal that states, "To Be Determined" (TBD) for a proposed Key Person, or omits a Key Person, will be rejected by the Government.

b. Letters of Commitment: The offeror shall provide a Letter of Commitment (**Section J, Attachment X**) for each proposed Key Person, at the proposal Part II submission due date. To meet this Pass/Fail criterion, the letter shall be signed by the proposed Key Person and shall state that (1) the proposed Key Person named is employed by the offeror or subcontractor, or has an offer of employment from the offeror or subcontractor that the Key Person intends to accept in the event of an award being made to the offeror; and (2) the proposed Key Person is available and committed to begin work on the Project Start Date designated in Section L.3.

c. Section 508 Compliance: The offeror's written proposal shall include a statement, provided at the time of proposal Part II submission, indicating its capability to comply with Section 508 requirements throughout its performance of this TO in compliance with Section H.7.1.

d. Key Personnel Requirements: The offeror shall provide a statement that all Key Personnel meet the requirements of the Alliant 2 Contract, and that all Key Personnel meet the requirements of the TO, including security clearance requirements at time of proposal submission. The offeror shall provide a confirmation statement that all proposed Key Personnel possess the security clearance level required in Section H.4.1 and **Section J, Attachment V** (DD 254) of the TOR. The offeror shall also indicate the required security clearance level in the Project Staffing Plan referenced in Section L.6.1 and **Section J, Attachment R** of the TOR.

e. Shared Services Platform 1.0 Solution: The offeror shall provide a statement that their proposed approach and solution is in compliance with Section C.5.7.1 of this TOR.

f. Alliant 2 Awardee: The offeror shall represent that it is an awardee of the Alliant 2 Unrestricted Contract at the time of proposal Part II submission by providing a copy of its Alliant 2 basic contract award document and contract cover page.

L.5.2.9 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT. (TAB N)

The offeror must submit the completed FAR Provision 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, which can be found in **Section J, Attachment II**.

L.6 SUBMISSION OF THE WRITTEN TECHNICAL PROPOSAL (PART III)

Each offeror shall submit all information described in the following paragraphs. The offeror shall provide one original printed version, five paper copies, and one electronic copy, containing all

required sections of this Part. No thumb drives will be accepted. The Project Staffing Plan (**Section J, Attachment R**) shall only be provided as one original printed version and one electronic copy; additional hard copies shall not be provided.

Part III is the written Technical Proposal and shall contain the following (page limitations, if applicable, are indicated in the parentheses following each item):

a. Project Staffing Plan
b. Project Staffing Rationale (limited to four pages)
c. Key Personnel Qualification Matrix (KPQM) (limited to five pages for each Key Person)
d. Transition-In Plan (limited to ten pages)
e. Technical Assumptions (if any)
f. QMP (limited to ten pages)
g. Corporate Experience (limited to nine pages)
h. Video Technical Proposal Presentation Slides (separately bound). If the slides are not submitted by the proposal due date specified in the Cover Letter, they will not be evaluated.

L.6.1 PROJECT STAFFING PLAN

The offeror shall provide a Project Staffing Plan in accordance with the Project Staffing Plan Template contained in **Section J, Attachment R**. The submission shall contain all proposed individuals that will be working on this effort. All Key Personnel proposed shall be identified in the Project Staffing Plan and available to begin work immediately on the Project Start Date indicated in Section L.3 of this solicitation.

All non-Key Personnel shall meet the requirements of the Alliant 2 Contract. If the names of all non-Key Personnel are not known prior to offer submission, the offeror may indicate To Be Determined (TBD) in the Project Staffing Plan. The names of non-Key Personnel are the only identifiers that may remain unspecified in the Project Staffing Plan. The offeror shall supply all requested information for all proposed personnel regardless of whether a name or TBD is provided. The names of all non-Key Personnel that can be provided shall be provided. Information in the Project Staffing Plan provides a basis for the Government to determine the efficacy of the Project Staffing Plan in relation to the offeror's Technical Approach. If TBD is indicated for any non-Key Personnel, the offeror shall supply the offeror's proposed experience/certifications that would be needed to perform the proposed Technical Approach in that role. All qualification sections of the proposed Project Staffing Plan shall be completed uniquely for each person or TBD role provided.

The offeror shall include all proposed personnel in each performance period of the Project Staffing Plan, regardless of whether there are hours proposed for that person in that period to maintain consistency between each period of performance.

The offeror shall ensure there is consistency in the level of effort between the Project Staffing Plan provided in Part III and the Written Cost/Price Proposal provided in Parts I and II, being cognizant of rounding issues.

L.6.1.1 PROJECT STAFFING RATIONALE AND METHODOLOGY

The offeror shall provide a Project Staffing Rationale for the proposed project staffing solution presented in the Project Staffing Plan. The offeror shall describe its rationale for the proposed labor mix and level of effort to support each TOR task. The offeror shall also describe what factors drove its proposed labor mix and how its proposed staffing solution will accomplish the Government's objectives and requirements. If the offeror chooses to propose ancillary service labor categories (reference Section B.6.1.3 of the Alliant 2 contract), the offeror shall provide the rationale within this section of the proposal. The offeror shall also describe its methodology for hiring, retaining, and replacing appropriately qualified personnel during the life of this TO.

L.6.2 KEY PERSONNEL QUALIFICATION MATRIX (KPQM)

The offeror shall submit a KPQM (**Section J, Attachment S**) for each Key Person proposed relating the specialized experience identified in Section H.1 of this solicitation and the qualifications of the person or persons being proposed for that position. For those additional Key Personnel proposed, the offeror shall identify the specialized experience and the corresponding qualifications for this experience. The offeror shall represent the following:

a. All Key Personnel meet the requirements of the Alliant 2 Contract.
b. All Key Personnel meet the requirements of the TO, including security clearance requirements. The offeror shall provide a confirmation statement that all proposed Key Personnel possess the security clearance level required in Section H.1 of the TOR. The offeror shall also indicate the required security clearance level in the Project Staffing Plan referenced in Section L.6.1 and **Section J, Attachment R** of the TOR.

All Key Personnel requirements apply at the time of proposal submission, unless otherwise noted.

L.6.3 TRANSITION-IN PLAN

The offeror shall provide a Transition-In Plan that aligns with the requirements in Section C.5.2. The offeror shall include in the Transition-In Plan an approach that provides for a seamless transition from the incumbent to the new contractor (hereafter referred to as the offeror).

The Transition-In Plan shall identify the roles and responsibilities of the offeror including proposed schedule(s) and milestones to ensure no disruption of service. The Transition-In Plan shall also identify and discuss the roles and responsibilities of the incumbent contractor and information expected from the incumbent. The offeror shall also identify any actions the offeror assumes are the responsibility of the Government.

L.6.4 TECHNICAL ASSUMPTIONS

The offeror shall identify and address any assumptions affecting the technical proposal citing the component(s) of the proposal to which they pertain. All technical assumptions and Basis of Estimate assumptions shall be included in the technical volume. This shall include any non-Cost/Price information that serves as the basis of a Cost/Price assumption identified in the offeror's Written Cost/Price Proposal.

The Government reserves the right to reject any proposal that includes any assumption that adversely impacts the Government's requirements.

L.6.5 QUALITY MANAGEMENT PLAN (QMP)

The offeror shall identify its approach for ensuring quality in meeting the requirements of each task of the TO (i.e., not just the corporate generic quality control process). The offeror shall describe its methodology and approach for determining and meeting performance measures identified.

The QMP shall contain at a minimum the following:

a. Performance Monitoring Methods
b. Performance Measures
c. Approach to ensure that cost, performance, and schedule comply with task planning.
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO.
e. Government Roles
f. Contractor Roles

L.6.6 CORPORATE EXPERIENCE

The offeror shall provide Corporate Experience for three projects performed within the last five years (need not be completed) by the business unit that will perform this effort. One of the Corporate Experience references shall be the prime's direct experience as the prime contractor; the remaining references may be from the prime, its subcontractors or teaming partners. These three projects shall be **collectively** similar in size, scope, and complexity to the requirements identified in Section C. Collectively similar in scope and complexity is defined as the projects, when taken as a whole, are similar to the requirements identified in Section C; for example, one proposed Corporate Experience is similar to the work required in Tasks 4 and 7, another project that is similar to Tasks 6 and 8, and another reflects experience managing a complex multi-agency requirement. Collectively similar in size is defined as the sum of the average annual ceiling value of each proposed Corporate Experience project is similar to the total ceiling value of each year of this requirement. The Corporate Experience information must be submitted in the format provided in **Section J, Attachment I**. The offeror shall ensure that all of the POCs are aware that they may be contacted.

All three projects shall be contracts or orders for the performance of actual technical requirements. Master contract vehicles (e.g., Blanket Purchase Agreements (BPA), Indefinite Delivery/Indefinite Quantity (IDIQ) contracts) do not satisfy the Corporate Experience requirement unless submitted together with TO(s), awarded and performed under the master contract vehicle, that are collectively similar in size, scope, and complexity to this requirement. Furthermore, a project reference that consists of multiple TO references from a single master contract vehicle is acceptable only if the individual TO references are from the same client company/agency name and demonstrate interrelated requirements. Multiple TO references must include an individual contract/TO number, value, and period of performance.

L.6.7 VIDEO TECHNICAL PROPOSAL PRESENTATION SLIDES

The offeror shall submit one original printed version, five paper copies, and one electronic copy of the Video Technical Proposal Presentation slides in advance of the Video Technical Proposal Presentation. The Video Technical Proposal Presentation slides shall be separately bound from

all other parts of the written proposal. If the slides are not submitted by the proposal due date specified in the Cover Letter, they will not be evaluated. The Video Technical Proposal Presentation (Part IV) requirements are described in Section L.7.

Unobtrusive company logos or names can be inserted in any or all slides. Slides should be sequentially numbered in the lower right corner. Transition effects shall not be used. Each slide shall reference in the top right corner, the Section/subsection number from Section C and the Section F deliverable that is being described/discussed on the slide, where applicable.

L.7 SUBMISSION OF THE VIDEO TECHNICAL PROPOSAL PRESENTATION (PART IV)

Offerors that have not heard otherwise shall submit six electronic copies of the Video Technical Proposal Presentation containing the information required herein Section L.8. The Video Technical Proposal Presentation shall be held at the unclassified level.

The Video Technical Proposal Presentation will be used to assess the offeror's capability to satisfy the requirements set forth in the TOR.

Video Technical Proposal Presentation slides presented that differ from slides delivered with the Written Technical Proposal in Part III will not be evaluated.

While there will be a separate oral Q&A session scheduled (Section L.7.4), the offeror shall present its submitted Video Technical Proposal in a manner that is clear and complete.

L.7.1 VIDEO TECHNICAL PROPOSAL PRESENTATION PARTICIPATION AND CONSTRAINTS

The offeror shall identify all authors of the Video Technical Proposal Presentation by name and association with the offeror in the opening credits. Key Personnel introductions may be integrated into the video opening credits for clarity. Participation in the Video Technical Proposal Presentation shall be limited to the offeror's Key Personnel and no more than three additional corporate representatives of the offeror. An offeror's Key Personnel includes only those persons who will be assigned to the TO as Key Personnel as described in Section H.1. The three additional corporate representatives (e.g., CEOs, company presidents, or contract representatives) from the offeror may appear for an introductory role, but will not be allowed to deliver the content of the offeror's video presentation. Introductory remarks by any corporate representatives will not be evaluated, but will count toward the offeror's allotted Video Technical Proposal Presentation time. For the remainder of the video presentation, only Key Personnel shall present. Content presented by any non-Key Personnel will not be evaluated.

The offeror's video presentation shall not exceed 90 minutes. There is no limit to the number of slides that can be presented during the Video Technical Proposal Presentation within the allotted timeframe. Only those video presentation slides presented as part of the Video Technical Proposal Presentation will be evaluated. Any content presented after the time limit is reached and any slides over and above those presented during the video presentation will not be evaluated.

L.7.2 VIDEO TECHNICAL PROPOSAL PRESENTATION MEDIA

The Video Technical Proposal shall be in a presentation format. Generally, the visual of the Key Personnel presenting the content shall be visible and not obscure the slide. Limited use of

graphics will be allowed, such as zooming in to parts of the offeror's technical solution. During this time, the visual of the Key Personnel may be replaced with the name of the speaker. Limited use of animation for technical diagrams is allowable. The Government discourages the use of advanced video graphics or cinematic features as these will not be evaluated.

The offeror shall provide the presentation in one of three formats:

a. Blu-ray quality: H.264, 24 megabits per second (Mbps), file type: .MP4
b. Digital Video Disk – Read Only Memory (DVD-ROM) High Definition (HD) video quality: H.264, 24 Mbps, file type: .MP4
c. DVD (regular) quality: H.222/H.262, 9 Mbps, file type: .MP4

Please note, the Government does not have a preference as to which format offerors elect to use. Video Resolution is left to the offeror's discretion. Resolution quality is not rated in the technical evaluation. Submission of the entire presentation on a single, playable disk is preferred.

GSA FEDSIM uses Azend Group Corp Model#BDP-M1061, Sony Model#BDP-SX1000, and Blu-Ray Combo Model#SBC-06D2X-U video players to view video media. Offerors are encouraged to test video playback and compliance using the same models. As an alternative, the offeror may contact the CS at least one week prior to the due date of Proposal Part IV, Video Technical Proposal Presentation, to schedule a time in which the offeror can utilize one of FEDSIM's players to assess playability themselves. The CS will provide the video player to the offeror and the offeror will have no longer than 30 minutes to assess playability.

L.7.3 TECHNICAL PROPOSAL ORAL Q&A SESSION

The purpose of the oral Q&A session is to allow the Government to ask questions, as deemed necessary, that will serve to clarify to the Government, for evaluation purposes, the offeror's methodologies and approaches as proposed. It is the Government's intent to ask clarifying questions only to the extent deemed minimally necessary for the evaluators to sufficiently understand what is being proposed. The offeror shall be prepared to answer questions about the Video Technical Proposal Presentation and the Written Technical Proposal in the oral Q&A session. The oral Q&A session will be held at the unclassified level.

Attendance at the oral Q&A session is limited to the offeror's proposed Key Personnel and no more than three additional corporate representatives of the offeror. The offeror's Key Personnel shall be prepared to answer questions about Parts III and IV in the Q&A session.

L.7.4 TECHNICAL PROPOSAL ORAL Q&A SESSION SCHEDULING

The CO will schedule the oral Q&A session with the authorized negotiator or the signatory of the SF 33. Each offeror's oral Q&A session will be preliminarily scheduled by the CO and/or CS after receipt of Part I and will be confirmed after Part II is received and the CO determines that the offeror passed all of the Pass/Fail requirements.

The oral Q&A session will be held at facilities designated by the CO. The exact location and any other relevant information will be provided when scheduled. Time slots will be assigned randomly and may not be changed or traded. The Government reserves the right to reschedule any offeror's oral Q&A session at its sole discretion.

L.7.5 TECHNICAL PROPOSAL ORAL Q&A SESSION FORMAT

The offeror shall address any clarification questions posed by the CO or the TEB Chairperson. Although no stated time limit for the duration of the Q&A session will be imposed, for planning purposes, it is anticipated that the session should not last more than one hour. The CO and the TEB Chairperson will be responsible for ensuring the schedule is met and that all offerors are given the same opportunity to answer clarification questions.

The offeror shall bring bound printed copies of its Technical Proposal Parts III and IV to refer to throughout its oral Q&A session. The offeror shall not present any information to the Government other than answering the clarification questions posed. **Proposal revisions are not expected and will not be allowed.** The offeror may briefly caucus to coordinate responses to specific requests for clarifications. These brief caucuses may not last longer than five minutes before presenting the coordinated response.

The entire session will be documented by the Government. Upon completion of the Q&A session, the Government may caucus to formulate any additional clarification questions regarding the technical proposal**.**

L.7.6 PROHIBITION OF ELECTRONIC RECORDING OF THE TECHNICAL PROPOSAL ORAL Q&A SESSION

The offeror may **not** record or transmit any of the oral Q&A session. All offeror's electronic and recording devices shall be removed from the room during the oral Q&A session. The offeror is permitted to have a timer in the room during the oral Q&A session.

L.8 VIDEO TECHNICAL PROPOSAL PRESENTATION TOPICS

Within the Video Technical Proposal Presentation, the Government does not expect the offeror to provide a restatement of the information already submitted in writing in Part III. Instead, the offeror shall address this information under the topics provided. The Video Technical Proposal Presentation shall include the following topics and be organized in the following order:

a. Topic 1: Technical Approach
b. Topic 2: Management Approach

L.8.1 TECHNICAL APPROACH (TOPIC 1)

The offeror shall identify and describe the methodology and analytical techniques to be used in fulfilling the technical requirements identified in the TOR. The offeror should tailor the technical approach to achieve the requirements as identified in Sections C, F, H, and J. The offeror's proposal shall be relevant to this TOR and reflect an effective understanding of TOR requirements. The Technical Approach shall describe the following:

a. Meeting the goals, objectives, conditions, and task and subtask requirements, identified in Sections C, F, H, and J of the TOR. The methodology shall clearly identify the Technical Approach and how it will address the goals, objectives, conditions, and task requirements.
b. Approach to the design of the Shared Services Platform 2.0 (Section C.5.4 – Task 4 subtasks 4.1 through 4.4, Sections C.5.4.1 through C.5.4.4). The offeror shall describe their technical solution, tools, methodology, and techniques for the creation of Shared

Services Platform 2.0, including all capabilities addressed in CDM DEFEND F Initial SSC (**Section J Attachment BB**).

c. The offeror's technical approach to building, testing, and securing the Shared Services Platform 2.0. (Section C.5.5 Task 5 subtasks 5.1 through 5.3, Sections C.5.5.1 through C.5.5.3). The approach shall include the offeror's plan to efficiently and effectively work to obtain an ATO on the Shared Services Platform 2.0 (C.5.5 Task 5). The offeror shall describe its technical solution, tools, methodology, and techniques. Additionally, the offeror shall describe its expected timeframe and key milestones to achieve these tasks.

d. The offeror's technical approach to integrating agencies on the Shared Services Platform 2.0 (Section C.5.6, Task 6 subtasks 6.1 through 6.3, Sections C.5.6.1 through C.5.6.3). The offeror shall describe its technical solution, tools, methodology, and techniques. Note that for purposes of the proposal, the offeror need only address its integration approach for the Shared Services Platform 2.0.

e. The offeror's technical approach for taking over, maintaining, and performing operations of the Shared Services Platform 1.0 (Task 7, subtasks 7.1 through 7.4, Sections C.5.7.1 through C.5.7.4) while simultaneously developing and standing up the Shared Services Platform 2.0. The offeror shall describe its technical solution, tools, methodology, and techniques.

f. The offeror's approach to stakeholder engagement and how its methods will assist the Government with increasing agency adoption of the Shared Services Platform (Task 8, subtasks 8.1 through 8.3, Sections C.5.8.1 through C.5.8.3).

g. The offeror shall discuss the complexity of each task (Sections C.5.1, C.5.2, C.5.3, C.5.4, C.5.5, C.5.6, C.5.7, C.5.8 and C.5.9) and what role the Government will play in the contractor's solution to each task. In addition, the offeror shall address the dependencies between tasks (i.e., can they be performed or not performed without affecting other tasks).

h. The offeror shall discuss its plan and considerations for evolving the CDM Shared Services Platform 2.0. The offeror shall discuss its planned evolutionary upgrades and innovations to incorporate all CDM Capabilities into the Shared Services Platform 2.0. The offeror shall identify its planned changes to the CDM Shared Services Platform 2.0 environment and include descriptive rationale for the selection and addition, or replacement of CDM Shared Services Platform 2.0 components in order to make all CDM Capabilities available to supported Federal agencies.

L.8.2 MANAGEMENT APPROACH (TOPIC 2)

The offeror shall identify the management approach, techniques, and tools that the offeror shall use to accomplish the objectives and requirements identified in this TOR. The offeror shall tailor the management approach to achieve the requirements as identified in Section C. The Management Approach shall describe the following:

a. The offeror's approach for providing program management support, process management and control, project status and cost (to include planned versus actual expenditures) reporting, and program metrics. This shall include the offeror's approach to managing multiple concurrent agency implementations.

b. The offeror's management methodology for handling lines of authority and communication, organizational structure, and problem resolution.
c. The offeror's approach to risk management during the TO, and the planned actions to mitigate or eliminate risks.
d. The offeror's management approach, processes, and procedures to ensure that the SSC maintains relevance by keeping up with the latest tools, industry practices, and the cyber threat landscape.

L.9 SUBMISSION OF QUESTIONS

Offerors are requested to submit questions grouped by solicitation Section and make reference to the particular Section/Subsection number. Questions must be received before the date specified on the Cover Letter for receipt of questions using the format in **Section J, Attachment W**. **Questions or requests for extension submitted after the cut-off date will not be considered.**

Any information given to a prospective offeror concerning this solicitation will be furnished promptly to other prospective offerors as an amendment to the solicitation.

L.10 DELIVERY INSTRUCTIONS

The offeror shall deliver written proposals to and receive acceptance from the address and individual identified in the Cover Letter. Proposals not received by 11:00 a.m. Eastern Time (ET) on the date stated in the Cover Letter will not be considered.

M.1 METHOD OF AWARD

The Government anticipates awarding a TO to the offeror whose proposal is the most advantageous to the Government, price and other factors considered. Technical proposals will be evaluated based on the factors described in Section M.7. A cost and price evaluation will only be done for offerors with a technical proposal receiving an overall technical rating of ACCEPTABLE or higher. All evaluation factors other than cost or price, when combined, are significantly more important than cost. Award may be made to other than the lowest priced technically acceptable proposal.

This acquisition is being conducted under FAR 16.5. Principles and procedures of Subpart 15.3 do not apply. Accordingly, the Government reserves the right to do any or all of the following:

a. Award on initial proposals, without discussions.
b. Ask clarifying questions during the question and answer period of the presentations if needed. Clarification questions may include asking the offeror to clarify statements made during video presentations, if the contents of the video presentations warrant clarification. Clarification questions may include asking the offeror to clarify its written technical proposals. As a result, the Government may have communications with some, but not all, offerors; these communications, however, will be clarifications and not discussions. In these situations, the Government will consider the offeror's clarifying response(s) without allowing proposal revisions.
c. After an offeror has been selected for award based upon a best value determination, the Government may negotiate a final reduced price. The negotiations will include reductions in profit/fee with the offeror selected for award in order to achieve the absolute best value for the Government. The Government may make award based on initial offers received or the Government may make award after clarifications of some aspects of the proposal or discussions relative to price only.
d. Have communications, ask clarifying questions, request corrections relative to minor errors in the cost/price proposal, or request cost/price substantiating documentation to facilitate the Government's final evaluation of cost proposals with one or some offerors. These communications, clarifications, or requests for corrections or substantiating documentation will not materially change the offeror's proposal in terms of conformance to TOR requirements, constitute discussions, or materially change pricing.
e. FEDSIM does not incorporate proposals into any resultant award.

Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in proposals is prescribed in 18 U.S.C. 1001.

M.2 PASS/FAIL ELEMENTS

The Government will evaluate the following pass/fail elements. **A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the technical and cost proposal conducted by the Government.**

Pass/Fail Elements:
The following will be evaluated on a Pass/Fail basis:

a. The Government will reject any proposal that does not provide a name for each Key Person proposed at the proposal submission due date. A proposal that states, "To Be Determined" or TBD for a proposed Key Person, or omits a Key Person, will be rejected by the Government (Section L.5.2.8.a).
b. The Government will reject any proposal that does not provide a Letter of Commitment, signed by each proposed Key Person at the proposal submission due date (Section L.5.2.8.b).
c. The Government will reject any proposal that does not provide a Section 508 Compliance Statement (Section L.5.2.8.c).
d. The Government will reject any proposal where the offeror does not state that all Key Personnel meet the requirements of the Alliant 2 Contract, and that all Key Personnel meet the requirements of the TO, including security clearance requirements at the time of proposal submission (Section L.5.2.8.d).
e. The Government will reject any proposal where the offeror does not state that their proposed approach and solution is in compliance with Section C.5.7.1).
f. The Government will reject any proposal where the offeror does not represent that it is an awardee of the Alliant 2 Unrestricted Contract (Section L.5.2.8.f).

M.3 COST/PRICE PROPOSAL EVALUATION

The offeror's cost proposal (Section L.5, Parts I and II, Tabs A through L) will be evaluated to assess for cost realism and price reasonableness. Cost analysis will be performed on all prime contractors and major subcontractors with contract values over ten percent of the total contract value. The six-month extension period, authorized by FAR clause 52.217-8, will not be included in the total evaluated cost; however, it will be evaluated to ensure that the option is available for the unilateral exercise of the Government should an extension become necessary. The offeror shall not propose a price for the six-month extension. The CAF is not included in the price evaluation.

Costs that are excessively high or low (without sufficient justification) may be considered unrealistic and unreasonable and may receive no further consideration. Any proposal that is not within the total estimated CPAF cited in Section L.3 shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the offeror would like the Government to consider as the justification for the deviation from the range.

The Government will reject any proposal from the prime contractor that does not have a Government-approved purchasing system at the time of the proposal Part I submission due date. The Government will determine a prime contractor as non-responsible (and therefore ineligible for award) if the firm does not possess an adequate cost accounting system as determined by the cognizant Federal agency, applicable to the offeror's most current organizational structure, for properly allocating costs applicable to this cost-type contract at the time of the proposal Part I submission due date.

M.4 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

Tab F will be evaluated to assess whether or not an actual or potential OCI exists as defined by FAR Part 9.5. If an actual or potential OCI is identified that cannot be feasibly mitigated, avoided, or resolved in accordance with FAR Part 9.5, that offeror may be ineligible for award.

M.5 COST ASSUMPTIONS

The Government reserves the right to reject any proposal that includes any cost assumptions that may adversely impact satisfying the Government's requirements. The Government does not intend to incorporate proposals into any resultant award; any assumptions to that effect will be rejected.

M.6 OVERTIME AND EXTENDED BILLING HOUR PRACTICES

The Government reserves the right to reject any proposal that includes overtime or extended billing hour practices that adversely impact or affect the Government's requirements.

M.7 TECHNICAL EVALUATION FACTORS

The Government will evaluate technical proposals (Sections L.6, L.7, and L.8, Parts III and IV) based on the following factors:

Factor 1: Technical Approach including the information presented under the technical approach topic as part of the video technical proposal presentation (Section L.8.1) and Transition-In Plan (Section L.6.3) provided in the written technical proposal volume Part III.

Factor 2: Management Approach and Project Staffing including the information presented in the management approach topic as part of the video technical proposal presentation (Section L.8.2) and the QMP (Section L.6.5) provided in the written technical proposal volume Part III. Also including on the information presented in the Project Staffing Plan, Project Staffing Rationale and Methodology, and Key Personnel Qualification Matrix (Sections H.1, L.6.1, L.6.1.1, and L.6.2) provided in the written technical proposal volume Part III.

Factor 3: Corporate Experience (Section L.6.6).

The technical proposal evaluation factors are listed in descending order of importance. All three technical factors combined are significantly more important than cost. The Government will combine the results of the written and video submissions, including the Q&A responses, to arrive at a rating for the technical evaluation factors as a whole. The receipt of an evaluation rating of NOT ACCEPTABLE in any single factor will result in the overall proposal being determined NOT ACCEPTABLE and therefore ineligible for award.

METHODOLOGY. For this acquisition the term "methodology" is defined as the system of practices, techniques, procedures, and rules as required by this TO. This definition is based on the PMI Project Management Body of Knowledge (PMBOK). For the avoidance of doubt, the Government is seeking a coherent discussion of how the offeror proposes to meet its requirements, rather than a mere restatement of the requirements or a mere listing of what it proposes to do. The latter will not be deemed to constitute a methodology.

M.7.1 FACTOR 1: TECHNICAL APPROACH

The Government will evaluate the Technical Approach factor based on the clarity, relevancy and completeness of the approach and the degree to which the proposal meets the requirements of the TOR Sections L.6.3 and L.8.1 and includes innovative and efficient methodologies.

These elements are not subfactors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating. The offeror's Technical Approach will be evaluated based on the degree to which it reflects:

a. A comprehensive, effective, and efficient approach/methodology for meeting, integrating, and accomplishing the goals, objectives, conditions, and requirements of each task that encompasses all of the subtask requirements identified in Sections C, F, H, and J of the TOR.
b. The degree of effectiveness, efficiency, and comprehensiveness of the offeror's methodology for its approach to the design of the Shared Services Platform 2.0.
c. The degree of effectiveness, feasibility, and efficiency of the offeror's approach for meeting the task requirements for building, testing and securing the Shared Services Platform 2.0, including the efficiency and effectiveness of the offeror's plan to obtain an ATO. Also, the feasibility and efficiency of the offeror's timeline to achieve these tasks.
d. The degree of effectiveness and feasibility of the offeror's approach to integrating agencies onto the Shared Services Platform 2.0.
e. The degree of effectiveness, efficiency, and feasibility of the offeror's technical approach for taking over and performing operations of the Shared Services Platform 1.0 while simultaneously developing and implementing the Shared Services Platform 2.0.
f. The degree of effectiveness, efficiency, and feasibility of the offeror's approach for stakeholder engagement.
g. A clear and relevant understanding of the complexity of each task (Sections C.5.1, C.5.2, C.5.3, C.5.4, C.5.5, C.5.6, C.5.7, C.5.8 and C.5.9), the role the Government will play in the contractor's solution to each task, and the dependencies between those tasks.
h. The relevancy and comprehensiveness of the offeror's discussion of the Shared Services Platform future direction and innovations. Also the relevance and feasibility of future upgrades in terms of functionality, performance, any new IT products or replacement of existing CDM products.
i. The comprehensiveness, relevancy, and effectiveness of the offeror's Transition-In Plan (TOR Section L.6.3).

M.7.2 FACTOR 2: MANAGEMENT APPROACH AND PROJECT STAFFING

The Management Approach and Project Staffing will be evaluated to assess the degree to which it reflects an effective, efficient, feasible, and practical level of understanding of the operating environment in accomplishing the tasks and deliverables of this TO from a management perspective, in particular those areas described in Section L.8.2, with minimal risk and innovative and cost-effective ideas. The following are not sub-factors and will not be separately rated but will be evaluated as a whole to arrive at the factor-level rating. The offeror's Management Approach and Project Staffing will be evaluated based on the degree to which it reflects:

a. A sound approach for providing program management support, process management and control, and project status in an efficient manner in a program management environment with multiple concurrent agency implementations.
b. Clear lines of communication between the offeror's team and the Government for timely problem identification, mitigation, and resolution.
c. The degree of relevance, comprehensiveness, and efficiency of the offeror's risk management methodology during the TO.
d. The degree of relevance and feasibility of the offeror's approach to ensuring the SSC is up-to-date with applicable technologies, industry practices, and cyber threats.

The QMP will be evaluated to assess the completeness, relevancy and efficiency of the QMP as it relates to the TOR as identified in Section L.6.5 and reflects the offeror's plan to control and monitor quality during the entire TO period.

The Project Staffing Plan will be evaluated including the efficiency of the labor hours and labor category mix. The Project Staffing Plan will also be evaluated to assess the degree to which it complies with the requirements outlined in Section L.6.1, including the estimated hours and labor mix for Key Personnel and the experience, skills, and qualifications of the personnel proposed. The KPQM and Project Staffing Rationale and Methodology will be evaluated to assess the appropriateness and completeness of the experience, skills, and qualifications of the proposed Key Personnel identified in Section H.1. Key Personnel will also be evaluated to assess the currency and applicability of experience as it relates to Section H.1.

M.7.3 FACTOR 3: CORPORATE EXPERIENCE

The Corporate Experience factor will be evaluated based on an overall (i.e., taken as a whole) consideration of the following (these elements are not subfactors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating):

a. Corporate experience reflects/identifies experience on projects that are collectively similar in size, scope, and complexity to the requirements contained in Section C of the TOR.
b. Corporate experience reflects current experience and the offeror's roles and responsibilities are collectively similar in size, scope, and complexity to the requirements contained in Section C of the TOR.
c. Corporate experience reflects the offeror's approach to client support to include quality assurance, risk management, and maintaining effective lines of communication.

One of the three corporate experiences shall be the prime's direct experience as a prime contractor; the remaining references may be from the prime, its subcontractors or teaming partners. The Government will evaluate Corporate Experience provided from both the prime contractor and any subcontractors equally.

M.8 TECHNICAL ASSUMPTIONS

Offeror assumptions will be reviewed in the context of the technical factor to which they apply. The Government reserves the right to reject any proposal that includes any assumption that may adversely impact satisfying the Government's requirements.