REQUEST FOR QUOTATION (RFQ)

Audit and Inspections Documentation Tool (AIDT)

RFQ# 47J00023R0003

Issued to:

Contractors under NASA SEWP Government-wide Acquisition Contract (GWAC)

Issued by:

General Services Administration (GSA)

Office of Inspector General (OIG)

1800 F Street, NW

Washington, D.C. 20405

SECTION 1 – SUPPLIES OR SERVICES AND PRICE/COSTS

1.1 GENERAL

The offeror shall perform the effort required by this Task Order Request (TOR) on a firm-fixed basis only in accordance with the terms and conditions of this TOR, the NASA SEWP Government wide Acquisition Contract (GWAC) which the resulting task order will be placed. This acquisition is under **National American Industry Classification System (NAICS) code 511210 Software Publishers,** with a small business size standard of $35M. The Product Service Code (PSC) for this acquisition is D317, IT and Telecom Web Based Subscription. No set-aside will be used; however, small businesses are encouraged to submit quotes.

1.2 SERVICES AND PRICES

The offeror is required to price for a 5-year period of performance on a firm-fixed priced basis. The quoted prices must be equal to or less than the prices awarded in the offeror's NASA SEWP contract. All proposed prices must be for the contractor site and must clearly delineate the tasks, labor categories and prices (including discounts) under which work will be performed.

1.2.1 CONTRACT LINE-ITEM NUMBER (CLIN) TABLES

Section 1.2.1.1 contains the sample CLIN Tables and option periods for the task order requirements.

1.2.1.1 CLIN TABLES:

Contract Line Item Number	CLIN Description	Qty	Unit of Issue
CLIN 0001 XXXXX - XXXXX	Installation & Configuration Support	1	Each
CLIN 0002 XXXXX-XXXXX	Data Migration	1	Lot
CLIN 0002 XXXXX - XXXXX	User Licenses	200	Lot
CLIN 0003 XXXXX - XXXXX	Training for administrators	1	Lot
CLIN 0004 XXXXX-XXXXX	Training for staff	1	Lot
CLIN 0005 XXXXX - XXXXX	Software Maintenance	12	Month

Contract Line Item Number	CLIN Description	Qty	Unit of Issue
CLIN 0006 XXXXX - XXXXX	Customized Report Building (up to maximum of 10)	TBD	Each
CLIN 0007 XXXX -XXXXX	Maintenance for Existing Licenses (approx. 170 licenses)	12	Month

SECTION 2 – STATEMENT OF WORK (SOW)

2.1 BACKGROUND

The GSA OIG provides comprehensive coverage of GSA operations through program, financial, regulatory, and system-related audits and inspections. The GSA OIG Office of Audits conducts audits of GSA programs and operations, provides contract audit services to assist GSA contracting officials in carrying out their procurement responsibilities, and provides oversight of the annual audit of GSA's financial statements and GSA's information technology security program for Federal Information Security Management Act compliance.

The GSA OIG Office of Inspections objectively analyzes and evaluates GSA's programs and operations through management and programmatic inspections and evaluations that are intended to provide insight into issues of concern.

The GSA OIG has used an audit and inspection documentation software platform for over 20 years. However, the life cycle of the current software ends in 2025.

2.2 OBJECTIVE

The GSA OIG requires COTS software to replace its current software that will be used to document and manage its audits and inspections. The COTS software should have at least 3 years of audit or inspection usage.

The GSA OIG is also seeking services to: (1) install, configure, and support the new COTS software and (2) train users on all aspects of the new COTS software.

2.3 SCOPE

The General Services Administration Office of Inspector General (GSA OIG) is presenting the requirements to acquire commercial off-the-shelf (COTS) audit and inspection documentation software and related services. The audit and inspection documentation software will be used to

document and maintain information related to the GSA OIG's audits and inspections. The GSA OIG requires two separate and independent configurations of the documentation software for audits and inspections because the standards, workflow, and reporting needs are different and unique to each other.

2.4 SOFTWARE REQUIREMENTS

2.4.1 Dashboards

a. General Dashboards

The configured software shall have:

i. Dashboards that are customizable by the user.

ii. Dashboards that summarize project universe information. For example, a dashboard that would summarize information from all projects within a given time frame or project status based on milestones or phases (planning, fieldwork, reporting etc.) and direct access to projects.

iii. Dashboards that indicate project-level information including completion and review status, visual cues on project progress, and direct access to items.

2.4.2 Distinct Projects

a. Permissions, Attributes, and Schedule

The configured software shall have:

i. Self-contained projects with unique permissions and roles. Role-based permissions determine type/level of access to the projects.

ii. Unique identifier for each project.

iii. Ability to record planned and multiple iterations of revised and actual milestones with explanations of revisions to establish and track a schedule for each project.

b. Project Browser

The configured software shall have:

i. Ability for users to see, access, and filter projects by project information. Project information includes title, project number, date initiated, status of the project, and standard milestones.

ii. Ability for the user to use various search terms to find and access a project (project title/project number).

2.4.3 System Configurability and Centralized Management

The configured software shall have:

a. User-friendly, intuitive, graphical user interface following industry standard best practices, allowing users to easily navigate the software after training.
b. Ability to create multiple project templates to allow for centralized policy management and ensure new projects include all required information, based on their type.
c. Ability to revise project templates.
d. Ability to create new, unique projects.
e. Ability to create, assign, and change permissions at a global and project level based on user roles such as administrator, reviewer, preparer, or combination of roles. This will allow centralized policy management by the GSA OIG.
f. Ability to create administrator accounts to perform administrative tasks in all projects.
g. Ability to create and use separate user accounts for performing system administration actions.
h. Ability to assign staff to different projects with permissions specific to each project.
i. Ability to copy existing projects to create new projects.
j. Ability to copy parts of existing projects and incorporate them into new projects.
k. Ability to customize data fields captured in the projects that can be globally reported.
l. Multiple configurable fields and labels for project information. Examples include project objective, fiscal year completed/expected to be completed, project milestones, project status, project findings including monetary impact (questioned costs/funds be put to better use), report recommendations, number of recommendations, whether client concurred or non-concurred with recommendations, and status of recommendation.
m. Ability to make a project read-only once it is complete so no additional changes can be made.
n. Ability to indicate that a project has been completed.
o. Ability to mark a project as cancelled or suspended and restrict access to read-only. Ability to reverse cancellation or suspension as needed.
p. Ability to generate and delete projects for training purposes.
q. Ability to delete projects.
r. Ability to add or delete users.
s. Ability to create project(s) from migrated data.

2.4.4 Project Documentation

The configured software shall have:

a. An automatic numbering/labeling system for items stored in the project to ensure items can be easily identified, linked, and located.
b. Ability to document audit and inspection work to include, but not limited to, the following areas: title, purpose, source, scope, and conclusion.
c. Ability to interact with Microsoft Office file types (including Word, Excel, and PowerPoint) and Adobe Acrobat PDF files including editing and saving.
d. Ability to interact with alternative file types (Google Docs, open-source files, etc.) and industry-standard media files (audio, video, image, etc.).
e. Ability to update, replace, and delete items.
f. Ability to assign items to users.
g. Ability to revise audit and inspection documentation names as needed.
h. Ability to provide visual status of items. Examples of statuses could include in-progress, prepared, and reviewed.
i. Ability to export/import items.
j. Ability to copy items from within a project and from one project to another.
k. Ability to export electronic form of unique audit and inspection software format (like an electronic form with multiple tabs/custom fields) to Microsoft and Adobe products.
l. Ability to support and store a high volume of items and large individual file sizes. As a reference point, the existing data repository is roughly 1TB with 500,000 documents and 2,500 projects. Individual projects typically range from 150MB on the low side to over 10GB on the higher side with files ranging from a few KB of data to over 1GB.
m. Ability to set items to read-only to prevent changes.
n. Software controls to mitigate risk of inadvertent loss of audit and inspection work at individual user levels (auto save functions).
o. Ability to recover deleted items in original form.
p. Ability to add visual cues indicating verification of statements and figures (e.g., tick marks) in documentation.
q. Ability to track and monitor user access and all events and actions related to project files and documentation.

2.4.5 Electronic Linking

The configured software shall have:

a. Ability to link items in the project file. For example, create links between Microsoft Word, Excel, PowerPoint, and PDF files and other formats unique to the software as well as to other areas of the project.

b. Ability to conduct cross-indexing/cross-referencing. This functionality shall include the ability to link a statement in a Microsoft Word document to a specific point in any item contained within the project.
c. Ability to efficiently handle a large number of links within individual items and across the project.
d. Ability to document findings/recommendations within a project and link them to supporting items.
e. Ability to create numerous links within individual items and across a project.

2.4.6 Findings and Recommendations

The configured software shall have:

a. Ability to create and document multiple findings per project based on audit and inspection work.
b. Ability to create multiple recommendations per finding.
c. Ability to create custom fields for findings (such as condition, criteria, cause, effect, and multiple fields for monetary impact) to support tracking and reporting requirements.
d. Ability to create custom fields for recommendations (such as staff office the recommendation was addressed to, whether the agency concurred with the recommendation, functional area that recommendation applies to, and date for recommendation resolution) to support tracking and reporting requirements.
e. Ability to update custom field entries.
f. Ability to link findings to supporting items.

2.4.7 Review Process for All Project Documentation

The configured software shall have:

a. Ability for preparer(s) to sign-off on items in projects and record when each sign-off occurred (preparer name, role, date, and time) including multi-level preparer sign-offs.
b. Ability for reviewer(s) to sign-off on items and record when each sign-off occurred (reviewer name, role, date, and time) including multi-level reviewer sign-offs.
c. Ability for preparer or reviewer to remove sign-off or edit items prior to or after supervisory sign-off, and ability for preparer(s) and reviewer(s) to sign-off again after edits.
d. Controls to prevent preparer from signing off as reviewer on items they created.
e. Ability to provide reviewer comments to multiple recipients and receive responses from preparer(s) and maintain a complete record of the correspondence.

f. Ability to update reviewer comments with additional comments and maintain a complete record of the correspondence.
g. Ability for preparer to indicate that a comment is ready for review.
h. Ability for reviewer to indicate that a comment is complete/reviewed.
i. Ability to link reviewer comments to associated items. Links will take recipient to the applicable location in the associated items.
j. Ability to sort and apply multiple filters to view reviewer comments including date comment was written, status of comment (needs to be addressed, ready to be reviewed, or reviewed), author of comment, and who the comment is directed to.
k. Ability to create reviewer comment summaries/reports based on various filters.
l. Ability to export reviewer comments, preparer responses, and sign-off dates/times.
m. Ability to provide peer-to-peer comments.
n. Ability to identify documentation and track changes in documentation that has been altered after supervisory review.
o. A log that shows edit dates and times, preparer sign-off dates and times, and reviewer sign-off dates and times of all items.
p. Ability to create notifications within the system for user-defined triggers such as pending deadlines, review status, recommendation dates, and required actions.
q. Ability to create email notifications based on user-defined triggers.

2.4.8 Sensitive Personal Information/Personally Identifiable Information Tags

The configured software shall have:

a. Ability to flag audit and inspection documentation as sensitive in a project.
b. Ability to restrict access to sensitive items in a project.
c. Role-based access control to sensitive items in a project.

2.4.9 Retention/Archiving/Storage

The configured software shall have:

a. Ability to support GSA OIG records management requirements.
    i. Ability for system to assign retention period based on cutoff (i.e., completion of project or closeout date), to permit the timely disposal or transfer of completed projects in accordance with National Archives and Records Administration (NARA)-approved retention schedules and NARA-approved formats.
    ii. Ability for system to generate ad hoc reports on project status, closeout dates, disposition notifications, etc.

b. Ability to delete project files and system documentation (in accordance with NARA-approved retention schedules) in a manner that keeps any protected information from being reproduced or recovered.
c. Ability to extract and transfer projects that require permanent preservation to NARA.
d. Ability for staff to access projects completed by other teams and to extract documentation and associated metadata.
e. Ability to archive completed projects.

2.4.10 Search Functionality

The configured software shall have:

a. Ability to search the project for specific terms within items including metadata tags such as document markings.
b. Ability to filter search results.
c. Ability to perform full-text search of contents within project documentation and associated metadata.

2.4.11 Miscellaneous Project Features

The configured software shall have:

a. Ability to format project documentation using features including:
    i. Support for rich formatting of text.
    ii. Support for copy/cut/paste with and without retained formatting.
    iii. Support for in-line and on-demand spell check, with editable dictionary.
    iv. Ability to create and format tables and graphs.

2.4.12 Offline Working Mode

The configured software shall have:

a. Ability to make changes to a project while offline.
b. Ability to cancel offline items locked by users who may no longer be using them.
c. Process to synchronize offline changes to locally stored data automatically to the GSA OIG network or cloud when internet is restored.
d. Ability to review and resolve conflicts from offline changes.
e. Controls to prevent unintentional overwrites by conflicting offline changes.
f. Ability for peer review access of entire project without access to the GSA OIG network or cloud.

2.4.13 Data Migration

The configured software shall have:

a. Ability to migrate project metadata and supporting files into the software by either:
    i. Direct import of project metadata by project or database from existing audit software.
    ii. Application programming interface (API) support to enable data migration by means of a data migration project.

2.4.14 Providing Project Documentation to External Parties

The configured software shall have:

a. Ability to export all data in the original structure related to a project including but not limited to documents and metadata in a format so that it can be accessed by external parties without requiring the purchase of additional software licensing.
b. Metadata may include but not be limited to electronic links between items, preparer and reviewer sign off histories, reviewer comments, users assigned to the project, and flags/identifiers associated with items.

2.4.15 Infrastructure

The configured software shall have:

a. Ability to support up to 200 concurrent users in multiple locations and time zones.
b. Ongoing support services including but not limited to security updates, patches, bug fixes, and any compliance and compatibility related issues.
c. Ability to test patch/upgrades prior to installation in a production environment.
d. Ability to extract all data from the cloud, if applicable.
e. Compatibility with Microsoft Office 365 and Adobe Acrobat DC and above.
f. Compatibility with alternative file types (Google Docs, open-source files, etc.) and industry-standard media files (audio, video, image, etc.).
g. Ability to monitor and report on performance metrics including but not limited to slow-moving or hung jobs/workflows, excessive memory consumption, and excessive central processing unit (CPU) use.
h. Performance that meets or exceeds industry performance standards when running on virtual machines and/or Virtual Desktop Infrastructure (VDI).
i. Support for single user sign-on/personal identity verification (PIV) cards. Ability for integrations of system access control (login/ windows authentication) through GSA OIG's active directory.
j. Support for SAML 2.0 or OIDC authentication with Azure Active Directory as Identity Provider.

k. Ability to handle slow or latent connections through virtual private networks or remote connections, including maintaining user session during large file uploads.
l. Ability to meet or exceed 95 percent user availability with the following downtime expectations:
    i. Daily: 1h 12m
    ii. Weekly: 8h 24m
    iii. Monthly: 1d 12h 13m 27s
    iv. Quarterly: 4d 12h 40m 22s
    v. Yearly: 18d 2h 41m 28s

2.4.16 Security/Hosting

The configured software shall have:

a. Ability to capture and report full logging of user activity, including deletions.
b. Ability to access logs and activity reports using industry standard best practices.
c. Federal information processing standard (FIPS) 140-3 certified cryptomodules for all encryptions. Contractor must provide the National Institute of Standards and Technology validation certificate number from https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules wherever contractor uses encryption anywhere in the system.
d. Encryption of data at rest and data in transmission when the software itself is safeguarding data including but not limited to user data, application data, network traffic, and authentication.
e. Ability for every user session to display a logon/warning banner with end-user acknowledgement to proceed.
f. Audit and inspection documentation software that can be provided via one of these options:
    i. On-premise at a GSA OIG data center location or
    ii. Cloud-based and hosted by GSA OIG or
    iii. Cloud-based and hosted by the contractor.
g. The system must meet all applicable federal government requirements including:
    i. Federal Information Security Management Act (FISMA) requirements;
    ii. National Institute of Standards and Technology (NIST) information security policies, procedures, and standards;
    iii. Federal Risk and Authorization Management Program (FedRAMP) certification for cloud-based software; and
    iv. OIG-specified requirements.
h. In compliance with OMB Directive M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, the vendor shall provide a self-attestation that serves as a “conformance statement”

described by the NIST Guidance. The NIST Secure Software Development Framework (SSDF), SP 800218,3 and the NIST Software Supply Chain Security Guidance4 (these two documents, taken together, are referred to as "NIST Guidance"

i. An acceptable self-attestation must include the following minimum requirements:
   - The software producer's name;
   - A description of which product or products the statement refers to (preferably focused on the company or product line level and inclusive of all unclassified products sold to Federal agencies);
   - A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form;
   - Self-attestation is the minimum level required; however, agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in M-21-30.

ii. A third-party assessment provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by the agency shall be acceptable in lieu of a software producer's self-attestation, including in the case of open-source software or products incorporating open-source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.

2.4.17 Operational

The configured software shall have:

a. Client applications that are configurable to work seamlessly on all devices regardless of operating systems or operating environment.
b. Ability to capture and effectively process all error conditions and provide detailed notice of recovery actions. The system shall resume operations, even if limited, after encountering an error.
c. Ability to provide, or leverage, existing identity-management services to support system administration capabilities to manage users and groups, where applicable, including creation, provisioning, permissions, etc.
d. Adherence to Section 508 of the Rehabilitation Act of 1973.
e. If the software is browser-based, then it must conform with NIST SP 800-52 Revision 2 or later.
f. Authentication and other traffic must comply with applicable NIST standards and any OIG-specified requirements.

g. Compliance with NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems*.
h. Ability to support the configuration of open protocol standards for the transmission of internet protocol-based communication flows.
i. Capability of running on a 64-bit operating system.
j. If the software is on-premise and relies on an external database product, then it must support Microsoft structured query language (SQL) Server 2016 or newer.
k. If the software is on-premise, the ability to support the latest GSA OIG-approved Microsoft Server Operating System Environments (OSE).
l. If the software is on-premise, the ability to be hosted on a VMWare virtual platform.
m. If the software is on-premise, the ability for the software to be extracted and moved via VMWare virtual container to a new data center or hosting location.
n. A flexible backup architecture in terms of frequency and types of data being backed up.
o. Ability to integrate with the GSA OIG's Active Directory/Lightweight Directory Access Protocol (LDAP) infrastructure if on premise, and Microsoft Azure Active Directory SAML/OIDC identity provider if cloud hosted.
p. Ability to perform diagnostic logging for the entire system (e.g., system logs, network access logs, and performance logs to help in troubleshooting the system and verifying security) including any virtual or physical hosts and associated infrastructure environment.
q. Support for secure remote administration of the system.
r. Capability of centralized management.
s. Ability to support high availability features, including, without limitation, clustering and load balancing.
t. Ability to include customizable role-based access.
u. Ability to provide a web-based, graphical user management console, for interacting with the system supporting GSA OIG-approved browsers.
v. If the software is on-premise, the ability to support IPv6.
w. Separation of user functionality (including user interface services) from information system management functionality.
x. Ability to disable user identifiers after 90 days of inactivity.
y. Ability to isolate/segregate data, in a multi-tenant environment, for cloud-based software.
z. If software is on-premise, the vendor must provide technical hardware specifications and any additional software specifications including licensing requirements needed to support the software.
aa. Contractor's technical and customer support websites/portals shall be hosted in the United States of America.

2.4.18 Incident Management

The configured software shall have:

a. The ability to capture and raise application events and security access attempts and send electronic notifications for identifying, submitting, and tracking incidents.
b. Integrated incident management software that helps track and respond unexpected user problems or questions that may occur.
c. An automatic incident report response, generating an incident number for user reference and a 24-hour response time to resolve issues effectively and efficiently.

2.5 IMPLEMENTATION AND CONFIGURATION REQUIREMENTS

2.5.1 Implementation and Configuration

a. Implementation

The contractor shall:

i. Provide an Implementation Plan that outlines the steps and time frames that will be followed to implement the software including, but not limited to, implementation working discussions, installing software, user access to software, and delivery of software.
ii. Provide a Quality Control Plan to ensure services are performed in accordance with this SOW. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services.
iii. Provide a Project Schedule outlining each major task and subtasks in conjunction with the requirements in this SOW.
iv. Provide Status Reports as defined by contract requirements and frequency as agreed to by both parties. The GSA OIG reserves the right to request a status update at any point during project duration.
v. Engage in regular communication and facilitate project-specific meetings, creating detail briefing materials and record, distribute, and archive reports and meeting minutes. Meeting minutes and action items shall be sent within 2 business days.

b. Configuration

The contractor shall:

i. Provide a Configuration Plan that outlines the steps that will be taken to configure the software to the GSA OIG's requirements including, but not limited to:
    1. Setting up rules and policies;
    2. Customizing access and user or group security roles and associated rights;
    3. Developing and implementing any specific global/universal terminology;
    4. Developing and implementing project templates and reports;
    5. Setting up groups for access to project data and information;
    6. Generating customized dashboard views for project and overall GSA OIG performance tracking;
    7. Configuring all custom fields available within the software; and
    8. Conducting Working Sessions together with GSA OIG administrators to perform baseline software installation and configuration.

ii. Coordinate and conduct a software demonstration of the software after the baseline software implementation and configuration is completed.

iii. Provide a Baseline Software Installation and Configuration Guide that details the software configuration to allow GSA OIG IT personnel to repeat the installation and configuration.

2.5.2 Technical and Customer Support

The contractor shall:

a. Provide software maintenance and technical support for the term of contracted software licensing and service, upon the GSA OIG's acceptance of the final configured software. The Technical Support Agreement should include the following support requirements, at a minimum:
    i. The contractor shall provide all software revisions and their base installation as part of the support agreement.
    ii. The contractor shall provide a scheduled software release cycle for software updates to provide major releases, service pack releases, and hotfixes at no additional cost to the government. Vendor shall provide a patch or mitigation within 30 calendar days for published vulnerabilities with a common vulnerability scoring system) (CVSS) version 3.0 score between 7.0 and 10.0 (reference criteria at the National Vulnerability Database: https://nvd.nist.gov/vuln-metrics/cvss)
    iii. The software shall have a documented contractor commitment to be at least 5 years away from end of life and shall have at least 5 years of customer support available.

b. Provide customer support services for the term of the contracted software licensing and service upon the GSA OIG's acceptance of the final configured software. The Customer Support Agreement should include the following requirements, at a minimum:
    i. Technical and customer support from the vendor during normal business hours Monday through Friday.
    ii. The contractor shall support emergency technical and customer support requests outside of normal business hours.
    vi. If the contractor is directly supporting the operation and maintenance of the software, then the contractor shall offer at least one tier of service that meets or exceeds 95 percent availability with the following downtime expectations:
        - Daily: 1h 12m
        - Weekly: 8h 24m
        - Monthly: 1d 12h 13m 27s
        - Quarterly: 4d 12h 40m 22s
        - Yearly: 18d 2h 41m 28s
    iii. The contractor shall provide a dedicated account manager.
    iv. The contractor shall conduct a Transition to Support Meeting to ensure GSA OIG designated representatives have knowledge on the support process.

2.5.3 Training

a. Training Plan

The contractor shall:

i. Develop a detailed Training Plan that covers how all aspects of training on the final configured software will be completed. The Training Plan shall include, at a minimum, detail on the following items:
    1. Itemized list of the user manuals to be provided.
    2. Contents to be included within the user manuals.
    3. List of different training sessions to be completed and tentative dates.
    4. Agenda that outlines topics that will be covered during each training session.

b. Training Materials

The contractor shall:

i. Provide all materials including but not limited to recordings, slides, and handouts that will be used during training sessions.
ii. Provide user manuals that detail all areas of system usage.

iii. Provide technical manuals that allow for system administration and describe all system components, user modification, and all necessary steps to enable the effective and efficient use of all system features.
iv. Provide all operation and maintenance manuals associated with the system.

c. Training Sessions

The contractor shall:

i. Provide role-based training with customized sets of training materials and sessions. The specific training session content will be agreed upon as part of the Training Plan. The different types of training sessions will include (but not be limited to) the following:
   1. GSA OIG Users
   2. GSA OIG Administrators

2.5.4 Additional Services

a. Customized Reports

The contractor shall:

i. Provide customized reports. There will be multiple customized reports that shall be defined and configured as part of this effort. While some reports are likely to be available with the base software, it is expected that customized reports will need to be created throughout the life of the contract. The specific requirements for each report and number of reports will be communicated to the contractor when needed. The contractor shall build these custom reports without access to the GSA OIG system or to any GSA OIG-sensitive information.
ii. The preliminary requirements for customized reports will be discussed at the Kickoff Meeting.
iii. The contractor shall build the customized reports, provide instructions on how to create the reports, and train GSA OIG administrators on how to maintain and modify the reports for future use.

2.6 GOVERNMENT FURNISHED EQUIPMENT (GFE) AND RESOURCES

The GSA OIG will provide government furnished equipment, government furnished information, and government furnished software for existing systems as deemed appropriate to accomplish the requirements under this contract.

2.7 INHERENTLY GOVERNMENTAL FUNCTIONS

No inherently governmental functions as defined in Federal Acquisition Regulation (FAR) 2.101 and FAR 7.5 shall be performed by the offeror under this contract. Offeror employees shall not participate in any deliberations or meetings intended to exercise an inherently governmental function. All final determinations such as binding the United States to take or not to take some action, selecting program priorities, and providing direction to Federal employees shall be made by the government. The offeror shall immediately notify the Contracting Officer's Representative (COR) and the Contracting Officer (CO) if performance of an activity would result in the performance of an inherently governmental function.

2.8 NON-PERSONAL SERVICES

In accordance with FAR 37.101, this contract is a non-personal services contract in that the Offeror personnel rendering the services shall not be subject, either by the contract's terms or by the manner of its administration, to the continuous supervision and control of a government officer or employee. The offeror shall immediately notify the COR and the CO if, through contract administration, the actions of a government employee will result in the performance of a personal services contract.

SECTION 3 – DELIVERABLES AND PERFORMANCE

The development of deliverables includes review and input by the Government. The offeror will submit draft versions for government review. After review by the government and discussions between the government and the offeror, documents will be updated, and final versions delivered.

3.1 DELIVERABLES MEDIA

The offeror shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. The electronic copies shall be compatible with MS Office 2010 or later version.

3.2 DELIVERABLES SCHEDULE

The contractor shall prepare all deliverables and other contract documentation utilizing contractor resources. The term "deliverables" refers to anything that can be physically delivered outside of services and products procured.

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
Entire SOW	Kickoff Meeting	(Meeting/ Document)	Due 5 business days from contract award.	In accordance with (IAW) quality assurance surveillance plan (QASP)	COR
Entire SOW	Meeting Minutes and Action Items	(Document)	Due 2 business days from meeting occurrence or assignment.	IAW QASP	COR
Entire SOW	User Manuals	(Documents)	Due 5 business days from contract award.	IAW QASP	COR
Entire SOW	Technical Manuals	(Documents)	Due 5 business days from contract award.	IAW QASP	COR
Entire SOW	Operation and Maintenance Manuals	(Documents)	Due 5 business days from contract award.	IAW QASP	COR
2.5.1.a.i	Implementation Plan	(Document)	Draft plan due 20 business days from kickoff meeting. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
2.5.1.b.ii	Quality Control Plan	(Document)	Draft plan due 20 business days from kickoff meeting. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.1.iii	Project Schedule	(Document)	Draft schedule due 20 business days from kickoff meeting. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.2.a	Technical Support Agreement	(Document)	Draft due 5 business days after contract award. Final version is due 5 business days from written GSA OIG feedback.	IAW QASP	COR

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
2.5.2.b	Customer Support Agreement	(Document)	Draft due 5 business days after contract award. Final version is due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.1.a.iv	Status Reports	(Documents)	Mutually agreed upon frequency and time frame.	IAW QASP	COR
2.5.1.b.i.	Configuration Plan	(Document)	Draft plan due 20 business days from kickoff meeting. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.1.b.i.8	Working Sessions	(Meetings/ Services)	Mutually agreed upon format, frequency, and time frame.	IAW QASP	COR

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
Entire SOW	Baseline Software Implementation	(Service)	Implementation of baseline software to occur 30 business days from the approval of the Final Configuration Plan and Implementation Plan.	IAW QASP	COR
2.5.1.b.ii	Configured Software Demonstration	(Meeting/ Service)	Configured software to be delivered and demonstrated 10 business days from baseline software implementation. Changes to configuration demonstrated 5 business days from written GSA OIG feedback.	IAW QASP	COR
Entire SOW	Final Configured Software	(Service)	Final configured software to be delivered 5 business days from written GSA OIG feedback.	IAW QASP	COR

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
2.5.1.b.iii	Baseline Software Installation and Configuration Guide	(Document)	Draft guide due 2 business days after initial software configuration is complete. Final version is due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.2.b.iv	Transition to Support Meeting	(Meeting/ Document)	Mutually agreed upon time frame once the GSA OIG accepts the final configured software.	IAW QASP	COR
2.5.4.a	Customized Reports and Instructions	(Document/ Service)	Due 30 days after request from GSA OIG is submitted.	IAW QASP	COR
2.5.3.a	Training Plan	(Document)	Draft plan due 10 business days from completion of software configuration. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR

Ref. No.	Requirement	Format	Timeline/Deadline	Acceptance Criteria	GSA OIG POC
2.5.3.b	Training Materials	(Document)	Draft training materials due 15 business days after final training plan approval. Final version due 5 business days from written GSA OIG feedback.	IAW QASP	COR
2.5.3.c.1	Training Session – Users	(Service)	Mutually agreed upon format, frequency, and time frame.	IAW QASP	COR
2.5.3.c.2	Training Session – Administrators	(Service)	Mutually agreed upon format, frequency, and time frame.	IAW QASP	COR

SECTION 4 – INSPECTION AND ACCEPTANCE

4.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports and other deliverables under this task order shall be performed by the OIG COR at the address specified in paragraph 5.3.

4.2 SCOPE OF INSPECTION

4.2.1 All deliverables will be inspected for content, completeness, accuracy, and conformance to task order 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 task order. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

4.2.2 The government requires a period not to exceed 10 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

4.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the task order, the offeror's quotation, and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

SECTION 5 – DELIVERABLES AND/OR PERFORMANCE REQUIREMENTS

5.1 PERIOD OF PERFORMANCE

The period of performance for this task order shall be one-year base period and four 1-year option periods.

Base Period – October 1, 2023 – September 30, 2024

5.2 PLACE OF PERFORMANCE

Primary. The primary place of performance will be at the GSA OIG Central Office located at 1800 F Street, NW, Washington, D.C. 20405. The contractor may be required by the GSA OIG to travel to one or more GSA OIG field offices.

5.3 PLACE OF DELIVERY

All deliverables, correspondence and copies of invoices shall be delivered to the COR at the address below:

GSA OIG
ATTN: Thomas Short, COR
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 501-3104
Email: thomas.short@gsaig.gov

5.4 NOTICE REGARDING LATE DELIVERY

The offeror shall notify the COR, as soon as it becomes apparent to the offeror, that a scheduled delivery will be late. The offeror shall include in the notification for 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 offeror. Such notification in no way limits the government's right to any and all rights and remedies, including but not limited to, termination.

SECTION 6 – CONTRACT ADMINISTRATION DATA

6.1 CONTRACTING OFFICER'S REPRESENTATIVE

A. The CO will appoint a COR in writing for the task orders. The COR will receive all work called for by the task orders for the government and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to offeror personnel.

B. The COR is not authorized to change any of the terms and conditions of the contract or the task orders. Changes in the scope of work will be made only by the CO by a properly executed modification to the task order. Additional responsibilities of the COR include:

(1) Monitor the offeror's performance to ensure compliance with technical requirements of the task orders.
(2) Review and approval of progress reports, technical reports, etc., which require government approval.
(3) Verify and certify that the items have been inspected and meet the requirements of the task orders.
(4) Notify the CO immediately if performance is not proceeding satisfactorily.

(5) Ensure that changes in work under the task orders are not initiated before written authorization or a modification is issued by the CO.
(6) Provide the CO a written request and justification for changes.
(7) Furnish interpretations relative to the meaning of technical specifications and technical advice relative to CO approvals.
(8) Inspect and accept service and deliverables, including visiting the place(s) of performance to check offeror performance, as authorized by contract/task orders inspection clause on a non-interference basis. This may include, but is not limited to, evaluation of the following:

(i) Actual performance versus schedule and reported performance.

(ii) Changes in technical performance which may affect financial status, personnel, or labor difficulties, overextension of resources, etc.

(iii) Verification that the number and level of the employees charged to the task orders are actually performing work under the task orders.

(9) At the completion of the task orders, advise the CO concerning the following:

(i) All articles and services required to be furnished and/or performed under the task orders have been technically accepted.

(ii) Offeror compliance with patent rights and royalties clauses of the task orders.

(iii) Recommend disposition of any government-furnished property in possession of the offeror.

(iv) Verify proper consumption and use of government-furnished property by the offeror.

(v) Prepare a performance report detailing compliance with requirements, quality assurance, timely completion, and any problems associated with the task orders.

C. The offeror is advised that only the CO, acting within the scope of the task orders and the CO's authority, has the authority to make changes which affect task orders prices, quality, quantities, or delivery terms.

D. The COR will furnish technical advice to the offeror to provide specific details, milestones to be met within the terms of the task orders, and any other advice of a technical nature necessary to perform the work specified in the task orders. The COR shall not issue any instructions which would constitute a contractual change.

6.2 INVOICE SUBMISSION

The offeror shall submit invoices using the GSA Customer Self Service (VCSS) website at https://vcss.ocfo.gsa.gov/. To register to use the VCSS system, the contractor may contact:

(1) Send Original Invoice To:
USDA-OCFO
Financial Information & Operations Division
Financial Operations & Disbursement Branch
2300 Main Street - 2SE
Kansas City, MO 64108

6.2.1 INVOICE REQUIREMENTS

The offeror(s) shall provide the invoice data in spreadsheet form (MS Excel) with the elements as specified in their schedule contract. In order to be considered proper for payment, invoices shall be submitted in accordance with the following instructions:

(a) Invoices shall be submitted monthly, unless otherwise specified, to the designated billing office specified in the resulting task orders.
(b) Invoices must include the Accounting Control Transaction (ACT) number provided on the resulting task orders.
(c) In addition to the requirements for a proper invoice specified in the Prompt Payment clause of the schedule contract, the following information or documentation must be submitted with each invoice:

- Contractor Name
- Contractor Address
- Contractor Point of Contact (POC) Name, Phone Number, and Email Address
- Contract Number
- BPA Number
- Task Order Number: *(From GSA Form 300, Block 2)*
- QP Number (ACT Number): *(From GSA Form 300, Block 4)*
- Invoice Number
- Period of performance covered by the invoice

- CLIN Titles
- CLIN Numbers
- Fixed Hourly Rate/Unit Price (by CLIN)
- Invoice Amount (by CLIN)
- Project Code (by Task or Subtask Area)
- Current Charges (by Project Code Number)
- Charges to Date (by CLIN)
- Total Invoice Amount

6.2.2 TRAVEL

No out-of-town trips anticipated but can be accommodated with justification. If travel is required, the government will negotiate travel expenses and authorize the travel in writing prior to the occurrence of travel. The contractor will submit travel requests no less than 10 calendar days prior to expected travel to the COR, who will review. Upon written approval, the contractor may be reimbursed. (Note: All travel is reimbursed in accordance with Federal Travel Regulation.) Travel vouchers will be submitted by the contractor no later than 3 business days after the contractor personnel have returned from travel.
Travel expenses shall be submitted on incident basis. Local travel will not be reimbursed.

SECTION 7 – SECURITY REQUIREMENTS

7.1 CONFIDENTIALITY AND NON-DISCLOSURE

a. Key Definitions

i. Information means: "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms." [Office of Management and Budget (OMB) Circular A-130 §10]

ii. GSA information means: information provided by GSA OIG or other GSA organizations.

iii. Sensitive information means: any GSA OIG information that would not be released to the public by GSA OIG under the Freedom of Information Act.

iv. Personally identifiable information (PII) means: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an

assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual." [OMB M-17-12 §III-B]

v. Record means: "all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them;" [44 U.S.C. §3301]

vi. System of records means: "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [5 U.S.C. §552a]

vii. Information system means: "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" [44 U.S.C. §3502]

viii. Information resources means: "information and related resources such as personnel, equipment, funds, and information technology" [44 U.S.C. §3502]

ix. GSA OIG system means: any automated data processing component serviced or maintained by GSA OIG, either connected or stand-alone.

x. Breach means: "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (a) a person other than an authorized user accesses or potentially accesses personally identifiable information or (b) an authorized user accesses or potentially accesses personally identifiable information for an other-than-authorized purpose" [OMB M-17-12 §III-C]

b. Confidentiality and Nondisclosure

Contractor acknowledges, understands, and accepts the following:

i. Presumption of sensitivity: Contractor shall presume that all GSA OIG information and information systems accessed while performing work under this contract are sensitive and must be protected as outlined in this Security requirements.

ii. GSA OIG property: Any GSA OIG information, software, applications, information systems and hardware accessed by contractor in the performance of work under the contract remain the sole property of the GSA OIG.

iii. Copyrights: To the extent that any software or applications on the GSA OIG information systems are protected by copyright, the contractor will not copy or disclose them without first obtaining the GSA OIG's prior written authorization, which will be provided only where authorized under applicable copyright law.

iv. Need to know basis: The contractor will access, or be provided access to, the GSA OIG information, software, applications, information systems and hardware only to the extent necessary, and only for performing the work required under the contract. The contractor will take reasonable steps to ensure that it will allow only those contractor personnel who need to see the GSA OIG materials to perform their work requirements have access. This paragraph also applies to any other GSA OIG information systems or information to which contractor may have access to or which may be disclosed to the contractor.

v. Restricted access: The contractor shall not authorize anyone other than those contractor personnel who require the information to perform work under the contract to access, disclose, modify, or destroy the information, software or applications on the GSA OIG information systems provided or accessed under the contract without the GSA OIG's prior written authorization. To the extent permitted by law, the contractor will refer all requests or demands for production of or access to GSA OIG information and information systems, including court orders, to the COR for response.

vi. Restrictions on copies: Except as authorized under the contract, the contractor shall not make any copies of any GSA OIG information provided to the contractor by the GSA OIG, including software or applications that are not copyrighted. Any authorized copies made by contractor shall be identified as GSA OIG information and protected as outlined in this Security Annex.

vii. Recording, sensitivity, and disclosure of GSA OIG information: Except to the extent necessary to perform the work under the contract, any information that contractor learns from and about GSA OIG information and information systems shall not be recorded and such information, whether recorded or not, shall be protected as outlined in this Security Annex. The contractor may not use or disclose this information except as the contractor is permitted to use or disclose under the User Agreement/Rules of Behavior and the Nondisclosure Agreement executed in accordance with this contract.

viii. GSA OIG Access to Information: The contractor will provide access to all information obtained or generated under the contract to GSA OIG employees as designated by the COR.

ix. Retention and return of information, software and equipment: Upon completion or termination of the contract for any reason, the contractor shall as soon as practicable, deliver all non-public (that is, not open to, shared with or otherwise made available to the public) GSA OIG information, copies made of GSA OIG information, software and equipment, in its possession, to the GSA OIG. The contractor shall not retain any copies of any GSA OIG sensitive/non-public information, software, or equipment unless authorized by the COR or by the GSA OIG Information Security Division.

x. Restricted disclosure: The contractor shall not disclose any GSA OIG information without prior consent from the GSA OIG. Disclosure of GSA OIG information to persons other than in the performance of the contract is authorized in only two situations: (a) pursuant to an order of a court of competent jurisdiction; or (b) with the GSA OIG's prior written authorization. Prior to any disclosure pursuant to a court order, contractor shall promptly notify the GSA OIG and provide the GSA OIG with a copy by fax or email, whichever is faster, and notify by telephone the COR in advance that it will be receiving such notices. The notice under this provision will include the following information to the extent that the contractor knows it, if it does not show on the face of the court order: the records to be disclosed pursuant to the order, to whom, where and when, for what purpose, and any other information that contractor reasonably believes is relevant to the disclosure.

xi. Notifications of unauthorized actions: The contractor shall promptly, within 1 hour of confirmation of an unauthorized action by contractor or contractor personnel, notify the COR and the GSA OIG Information Security Division of any access, disclosure, disposition, or destruction of GSA OIG information and information systems not authorized under the contract. To the extent known, contractor will notify the COR and the GSA OIG Information Security Division of the information improperly disclosed, to whom, how, when, the reason for the access, disclosure, disposition or destruction, and any other relevant information or information requested by the GSA OIG.

xii. Law enforcement and legal proceedings: The contractor will cooperate with the GSA OIG and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any unauthorized access, disclosure, disposition or destruction of GSA OIG information or property. The contractor will also cooperate with GSA OIG in any civil litigation to recover GSA OIG information or property, to obtain monetary or other compensation for a third party, or to obtain injunctive relief against any third party who accessed, modified, disclosed, or destroyed GSA OIG information and information systems except as explicitly authorized under the contract.

7.2 PERSONAL SECURITY

a. Mandatory GSA OIG User Agreement/Rules of Behavior and Nondisclosure Agreement

i. General rule: Every individual contractor personnel who will access GSA OIG information or GSA OIG information systems under the contract shall complete a GSA OIG User Agreement/Rules of Behavior (UA/RoB) and Nondisclosure Agreement (NDA) before obtaining access and starting work.

ii. Sign UA/RoB: Each individual contractor personnel who will access GSA OIG information or GSA OIG information systems under the contract shall complete the following tasks prior to the GSA OIG authorizing such access:

1. Read the current GSA OIG UA/RoB

2. Complete and sign it

3. Return the original signature page to the COR

4. The current GSA OIG UA/RoB will be provided by the COR.

iii. Sign NDA: Each individual contractor personnel accessing GSA OIG information or information systems under the contract shall complete the following tasks prior to the GSA OIG authorizing such access:

1. Read the current GSA OIG NDA

2. Complete and sign it

3. Return the original signature page to the COR

4. The current GSA OIG NDA will be provided by the COR.

iv. Sign annually: Should this contract be extended, each individual contractor personnel shall sign the UA/RoB and NDA annually and return it to the COR prior to accessing GSA OIG information or information systems and starting work, for each year of the contract.

v. Sign individually: Each individual contractor personnel shall individually sign the UA/RoB and NDA.

vi. Provide originals: Each individual contractor personnel shall provide an originally signed UA/RoB and NDA to the COR before the staff member accesses GSA OIG information or GSA OIG information systems. Copies, faxes, .pdf/image files, etc. are not permissible. Digital signatures using a non-repudiation certificate that is created by either a public certificate authority (CA) or use an in-house CA can be accepted if the GSA OIG Information Security Division determines the signature validates; however, the CA must appear on one of the Federal Bridge Trust List lists (https://www.idmanagement.gov/buy/trust-services/). If using an in-house CA, the GSA OIG ISD must pre-approve the contractor's CA and certificates proposed for digital signatures.

b. Initial Background Check

i. Contractor personnel shall pass an initial background check completed by the GSA OIG before beginning work. The GSA OIG facilitates an initial background check on each individual contractor personnel. To complete this background check, contractor personnel shall perform the following steps:

ii. Provide OF-306 form: Each individual contractor personnel shall provide a completed and signed OF-306 (Declaration for Federal Employment) to the COR. The OF-306 form is used for the suitability/background check process.

iii. Provide information: Each individual contractor personnel shall provide the following information about himself/herself to the COR:

1. Full legal name (first, middle initial, and last name; and prefixes and suffixes, if applicable)

2. Other names known by, such as maiden name, any alias, nicknames, etc.

3. Other names used

4. Social security number

5. Gender

6. Date of birth (month, day, year)

7. Place of birth (zip, city, and state or name of foreign country)

8. Citizenship

9. Current home address

10. Current phone numbers applicant can be reached at

11. Current Work address, supervisor name, and supervisor phone number

12. Current Work email address

13. Employment dates at the contractor

14. Previous employment history including city and state (7 years)

15. Previous home address history including city and state (7 years)

16. Currently active background investigation and/or suitability determination

17. Job title and position under this contract. The information should describe the:

a. Level of responsibility in the firm (e.g., partner, manager, etc.),

b. Division assigned to, and

c. Nature of the work assignment (e.g., financial or IT auditor, penetration testing specialist, actuary, economist, data specialist, etc.)

18. Should the GSA OIG require additional information for the performance of background checks, the contractor will work with the GSA OIG to obtain such additional information. The contractor shall provide the GSA OIG any additional requested information within 5 business days.

iv. Transmit information securely: The contractor's personnel security officer shall securely submit the information gathered to the GSA OIG in a format accepted or designated by the GSA OIG. The contractor's personnel security officer may provide the GSA OIG hard copies or use secure electronic submission. For electronic transmission, contractor will coordinate with the COR and the GSA OIG Information Security Division on acceptable methods.

v. Receive authorization to start: The GSA OIG will provide notice to the contractor of individuals approved to start work and access GSA OIG information or GSA OIG information systems. No contractor personnel shall commence work without GSA OIG approval.

vi. Annual updates: Should this contract be extended, contractor personnel shall follow the above procedures and obtain approval from the GSA OIG prior to accessing GSA OIG information or information systems and starting work, for each year of the contract. For team members who remain continuously on the engagement, the GSA OIG will notify contractor each year whether the required information needs to be resubmitted.

vii. Timing: The contractor shall incorporate into its project schedule sufficient time for the GSA OIG to complete initial background checks before members are scheduled to begin work. The initial background check generally takes 3 to 5 business days to complete.

c. On-Site Access; Personal Identity Verification (PIV) Card, Non-PIV card, and Badging

i. Site visit access: The contractor shall coordinate physical access requirements with the COR. Contractor personnel will be escorted at all times while at GSA OIG locations.

ii. PIV/badge requirements: If the contractor or GSA OIG require routine physical access to GSA OIG offices, the contractor shall follow GSA OIG physical access requirements including using a GSA-issued PIV/Non-PIV card or another badge where required. The GSA OIG will provide the additional contractual requirements if this applies.

iii. On-Site Access to Sensitive Information: Access provided under this section to GSA OIG locations that are not accessible by the public along with all sensitive information observable or heard in those non-public locations does not authorize contractor to create, capture, record, or retain any sensitive information unless using GSA OIG-authorized IT inventory.

d. **Keys and Physical Access Devices**

i. The contractor shall promptly (but no more than within 3 calendar days) return keys, access cards, access fobs, etc., provided by the GSA OIG. The contractor is responsible for reimbursing the GSA OIG for costs associated with failure to return access devices.

e. **Departure Notifications**

i. Termination or unplanned departure: The contractor shall notify the CO, COR, and GSA OIG Information Security Division immediately, but not more than one hour after discovery, of any termination or unplanned departure of personnel and provide written confirmation to the COR within 1 calendar day.

ii. Planned departures: Contractor shall notify the CO, COR, and GSA OIG Information Security Division with written confirmation of planned staff departures or planned removal from work under this contract within 15 calendar days of planned departure or removal.

iii. Departure confirmation: The contractor shall provide the COR with written confirmation within 3 calendar days confirming that the planned departures have occurred.

iv. Equipment of departed staff: The contractor shall coordinate with the COR on the reassignment or return of any GSA OIG-approved equipment from personnel leaving the engagement. No equipment shall be released from the contract without final sanitization approval from the GSA OIG Information Security Division.

7.3 TECHNICAL AND SECURITY CONTROLS

a. Contractor Access to and Use of Equipment, Devices, or Media for Contract Work

i. GSA OIG issued equipment: For this contract, the GSA OIG will issue equipment, devices, or media (collectively referred to as “IT inventory”). If contractor personnel already have GSA OIG-issued equipment, GSA OIG-issued PIV or non-PIV cards, or GSA OIG-provided Active Directory accounts, the GSA OIG Information Security Division will determine whether to authorize the previously issued GSA OIG resources for this contract.

ii. Work products: Work products (deliverables, notes, etc.) that are not sensitive information may be created, maintained, and stored on the contractor’s IT inventory. All sensitive information shall be created and maintained only on GSA OIG IT inventory. If the software is a contractor-managed FedRAMP authorized cloud, the contractor may maintain

sensitive information within the GSA OIG-controlled boundary of the FedRAMP cloud as directed by the GSA OIG.

iii. Transporting: The contractor is prohibited from transporting, shipping, or operating any contractor IT inventory outside of the United States of America that contains information obtained or created for this contract without permission from the COR.

iv. Connections: The contractor is prohibited from connecting contractor IT inventory to any non-public GSA OIG systems without explicit GSA OIG Information Security Division authorization.

v. Testing platforms: The contractor may establish, at contractor's cost, a test lab or environment for assessing deliverables. The contractor shall not import, process, or store any sensitive GSA OIG information (including sensitive security configurations or accounts) on the contractor's test environment. Use of a GSA OIG-hosted test lab or environment outside of the GSA OIG control requires explicit pre-approval by the GSA OIG Information Security Division.

vi. Non-OIG IT inventory: The contractor acknowledges and accepts that if any non-GSA OIG-provided IT inventory is proposed for use, the GSA OIG Information Security Division may require additional security measures be met to the satisfaction of the GSA OIG Information Security Division including, but not limited to, device configuration, infrastructure protection, and device/media sanitization before authorizing those devices or media. Sensitive information shall never be created on, transmitted to, accessed on, or stored on non-GSA OIG IT inventory including when consulting with other contractor personnel that are not approved for work under the contract.

vii. Hard copy media: Hard copy media, including but not limited to printing, of any sensitive GSA OIG information is prohibited unless explicitly authorized by the GSA OIG Information Security Division or COR.

viii. Phones: Contractor personnel may be permitted to use GSA OIG landline phones on a case-by-case basis but will limit long-distance/toll calls to essential business only. The contractor may use a personal or contractor-furnished landline or cellular phone for work under this contract if the contents of phone conversations are never recorded on any non-GSA OIG system.

b. File, Video, and Collaboration Services

i. Blocked sites: The GSA OIG generally blocks file sharing websites such as box.com, dropbox.com, and similar sites. The GSA OIG may block video streaming hosting sites and collaborative hosting sites. The contractor shall not be able to use any sites blocked by the

GSA OIG for work or for deliverables under this contract. The contractor accepts that GSA OIG cannot provide an exhaustive list of sites that the GSA OIG blocks.

ii. Sharing sites: The contractor will coordinate with the COR to use the GSA OIG's Teams or Webex capabilities to meet contract deliverables, including transmitting files or messages. Contractor will provide requests to the COR no less than 2 full business days before the GSA OIG's Teams access is required.

iii. GSA OIG-provided applications: GSA OIG-provided or contractor-hosted Microsoft Teams are authorized. GSA OIG-provided or contractor-hosted WebEx meetings are authorized. Other GSA OIG-provided services including but not limited to Office 365 applications will require advance approval by the GSA OIG Information Security Division.

iv. Collaboration Access to Sensitive Information: Access provided under this section to GSA OIG systems that are not accessible by the public along with all sensitive information communicated through such services does not authorize the contractor to create, capture, record, or retain any sensitive information unless using GSA OIG-authorized IT inventory.

v. Collaboration Access Restrictions: Contractor personnel are prohibited from accessing or joining any collaboration sites or sessions from outside the United States of America without explicit pre-authorization from the COR.

c. Electronic Mail (Email)

i. Contractor email: Contractor personnel will use GSA OIG email service for all email communications under this contract. Use of personal email accounts is prohibited.

ii. Email size: The GSA OIG limits the total size of individual emails. Proposed exchanges of messages + files greater than 10MB per email will use an alternative solution.

d. Assessment and Authorization (A&A)

i. Cloud-based software: Cloud-based software proposed under the contract must be listed as "FedRAMP Authorized" on https://marketplace.fedramp.gov. The GSA OIG will not provide Agency Authorization support for FedRAMP. GSA OIG Information Security Division staff must have full access to all FedRAMP documentation and artifacts – the GSA OIG Information Security Division usually requests this access directly via the FedRAMP.gov points of contact.

ii. Hardware or software: Hardware or software proposed under the contract must conform with federal security and privacy requirements including but not limited to PIV-based

or other GSA OIG-supported two factor authentication, FIPS 140-2 encryption certification, configuration, and continuous monitoring.

iii. A&A documentation support: The contractor shall provide authority to operate (ATO) documentation support to GSA OIG IT staff in completing A&A artifacts including but not limited to:

1. System Security Plan (SSP)

2. FIPS 199 Categorization Worksheet

3. Configuration Management Plan (CMP)

4. Contingency Plan (CP)

5. Incident Response (IRP)

6. Privacy Impact Assessment (PIA)

7. Privacy Threshold Assessment (PTA)

8. Rules of Behavior

9. System Boundary Diagrams (networking, data flow, authentication, etc.)

e. Reporting Security Incidents

i. Reporting incidents: The contractor shall report to the COR and to the GSA OIG Information Security Division any security incidents or allegations of violations by contractor personnel as soon as known, but not more than 1 hour after discovery. Following a verbal notification, contractor shall provide a written report within two business days or sooner, if requested by the GSA OIG.

ii. Reporting within GSA OIG facilities: When visiting a GSA OIG facility or any facility required under the contract, the contractor shall also report any security incidents as soon as known, but not more than 1 hour after discovery, to GSA OIG representative on site or the GSA OIG official coordinating the site visit.

iii. Security incident: A security incident is a violation of computer security policies, acceptable use policies, or standard security practices identified in the contract, including but not limited to:

1. Unauthorized access to, or disclosure of, GSA OIG information.

2. Unauthorized modification or destruction of GSA OIG information.

3. Reduced, interrupted, or terminated information processing capability.

4. Introduction of malicious programs or virus activity.

5. Degradation or loss of GSA OIG information system and/or confidentiality, integrity, or availability. This includes, but is not limited to, compromised passwords and failure to encrypt information when emailing or storing it.

6. Loss, theft, damage, or destruction of a GSA OIG asset or IT resource, or an individual contractor personnel's asset or IT resource that contains GSA OIG information, for example, loss of a laptop.

iv. Confiscation: Contractor and contractor personnel accept that the GSA OIG has the authority to confiscate any contractor equipment that either (1) store or transmit sensitive GSA OIG information but do not meet the GSA OIG's security requirements, (2) connect to non-public GSA OIG systems but do not meet the GSA OIG's security requirements, (3) are unauthorized in GSA OIG non-public areas, or (4) are used for illegal activities.

v. Reporting: The parties acknowledge that the GSA OIG must adhere to OMB Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" which establishes reporting requirements for government agencies.

f. Liability for Damages or Corrective Actions

i. Contractor liability: The contractor will be responsible for the actions of all individuals provided to work for the GSA OIG under this contract. As an independent contractor, the contractor shall be responsible for any costs incurred by the GSA OIG as a result of contractor negligence or corrective actions in response to liability claims. For example, the GSA OIG may incur costs to for notifying individuals of inappropriate disclosure of personal information. Furthermore, in the event that damages arise from work performed by contractor personnel under this contract, the contractor shall be responsible for all resources necessary to remedy the incident.

g. Liquidated Damages for Breach

i. Sensitive personal information: Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to the GSA OIG for liquidated damages in the event of a breach or privacy incident involving any sensitive personal information the contractor processes or maintains under this contract.

ii. Notice: The contractor shall provide notice to the GSA OIG of a "security incident" as set forth in the Security requirements. Upon such notification, the GSA OIG will conduct an independent risk analysis of the breach to determine the level of risk associated with the breach for the potential misuse of any sensitive personal information involved in the breach. The contractor shall fully cooperate with the entity performing the risk analysis. A report of a breach by itself is not interpreted as evidence that the contractor did not provide adequate safeguards. Failure to cooperate may be deemed a material breach and grounds for contract termination.

iii. Risk analysis: Each risk analysis shall address all relevant information concerning the breach, including the following:

1. Nature of the event (loss, theft, unauthorized access)

2. Description of the event, including:

a. Date of occurrence

b. Data elements involved, including any personally identifiable information (PII), such as full name, social security number, date of birth, home address, account number, disability code

3. Number of individuals affected or potentially affected

4. Names of individuals or groups affected or potentially affected

5. Ease of logical access to the lost, stolen or improperly accessed information in light of the degree of protection for the information (example: unencrypted, plain text)

6. Amount of time the information has been out of GSA OIG control

7. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons)

8. Known misuses of information containing sensitive personal information, if any

9. Assessment of the potential harm to the affected individuals

iv. Liquidated damages: Based on the determinations of the independent risk analysis, contractor shall be responsible for paying to the GSA OIG liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1. Notification

2. One year of credit monitoring services consisting of automatic daily monitoring of at least three relevant credit bureau reports

3. Breach analysis

4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution

5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible

6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs

h. Audit and Investigation

i. Audit or investigation: To the extent permitted by law, the contractor will cooperate in any audit or investigation related to this contract and project conducted by the GSA OIG.

ii. Cooperation: The contractor shall cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the GSA OIG as described in paragraph 3.h.i of this Security Annex including, but not limited to, prompt disclosure to authorized officials of information and records requested in connection with any audit, inspection, investigation, or review, and making employees of contractor available for interview by auditors, inspectors, and investigators upon request.

iii. Security incident: In the event of any security incident as defined in paragraph 3.e.iii of this Security Annex, including but not limited to those constituting an actual or potential threat or hazard to the integrity, availability, or confidentiality of GSA OIG information in the possession or under the control of the contractor or to the function of information systems operated by contractor in the performance of the contract, the contractor shall follow notification requirements addressed in paragraph 3.h.iv of this Security Annex, and shall preserve such GSA OIG information, records, logs and other evidence which are reasonably necessary to conduct a thorough investigation of the security incident.

iv. Prompt reporting: In the event of any security incident as described in paragraph 3.h.iii of this Security Annex, the contractor shall promptly, within 1 hour of the suspected or confirmed incident by the contractor, notify the GSA OIG Information Security Division about the incident. This notification requirement is in addition to any other notification requirements which may be required by law or by this contract. Established federal agency time frames for reporting security incidents to the United States Computer Emergency Readiness Team (US-CERT), although not exhaustive, serve as a useful guideline for determining whether reports under this paragraph are made promptly. (See NIST Special Publication 800-61, Appendix J). Contractor acknowledges that the GSA OIG must adhere to OMB Memorandum 17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information” which establishes reporting requirements for such security incidents.

v. Timely production of GSA OIG information: The contractor shall timely produce to the requestor (with the requestor being the COR, a representative of the COR, or the GSA OIG) GSA OIG information or records under the control of or in the possession of contractor pursuant to the contract, which the GSA OIG may request in furtherance of other audits, inspections, investigations, reviews or litigation in which GSA OIG is involved. Requests for production under this paragraph shall specify a deadline not less than 7 calendar days for compliance which will determine whether response to the request has been made in a timely manner.

vi. Storage: The contractor shall ensure that all storage of all GSA OIG information and records under the control of or in the possession of contractor pursuant to the contract are performed within the United States of America.

vii. Content capturing: In support of the investigation of security incidents as described in paragraph 3.h.iii of this Security Annex, as well as other investigations under the purview of GSA OIG, the contractor will maintain the capability to capture full-content network traffic between the Internet and any GSA OIG information systems operated by the contractor in the performance of the contract. When permissible under applicable law, the contractor shall initiate the capture of network traffic, if not already occurring, at the request of the COR, a representative of the COR, or the GSA OIG.

viii. No expectation of privacy: Contractor understands that users accessing GSA OIG-provided information systems operated by contractor or the GSA OIG in the performance of this contract have no reasonable expectation of privacy regarding any communications or information transiting or stored on GSA OIG-provided information systems. The contractor shall obtain consent from all users accessing GSA OIG-provided information and information systems maintained, operated, or used by the contractor under this contract, to monitoring and disclosure of any communications or information transiting or stored on these information systems for any purpose, by providing users with GSA OIG-approved network banners at all logins and points of access, and by incorporating such notice in its user terms of service as appropriate.

i. Contractor-Provided Inventory Restrictions

i. General Prohibitions: The contractor is prohibited from proposing or using foreign-sourced hardware, firmware, or software that is prohibited or blocked by federal law, federal regulation, or federal sanction including but not limited to:

1. Pub. L. 115-232 Section 889(a)(1)(A) [implemented in Federal Acquisition Regulation 52.204-24 and 52.204-25].

2. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

3. https://www.cbp.gov/trade/programs-administration/forced-labor/withhold-release-orders-and-findings

ii. Source Prohibitions: The contractor shall only use inventory that are obtained from a bona fide company incorporated within the United States. Companies that solely function as a reseller or rebrander but provides no further legal representation for manufacturers based in China do not meet this requirement.

iii. Gray Market: Used, refurbished, or remanufactured parts may be provided. No gray market supplies or equipment shall be provided. Gray market items are original equipment manufacturers (OEM) goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

iv. Counterfeits: No counterfeit supplies or equipment shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

v. Contractor Requirements: The contractor shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

7.4 Government Contacts

The following government personnel have been identified to support this Task order.

7.4.1 Contracting Officer (CO)

Emmanuel Osei Darko
General Services Administration
Office of Inspector General
Central Office
1800 F Street, NW
Washington, D.C. 20405
Email: emmanuel.oseidarko@gsaig.gov

7.4.2 Contracting Officer Representative (COR)

Thomas Short
General Services Administration
Office of Inspector General
Central Office
1800 F Street, NW
Washington, D.C. 20405
Email:thomas.short@gsaig.gov

SECTION 8 – CONTRACT CLAUSES

Clause No	Clause Title	Date
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.203-14	Display of Hotline Posters	(Dec 2007)
52.204-2	Security Requirements	(Aug 1996)
52.204-7	System for Award Management	(Oct 2018)
52.204-16	Commercial and Government Entity Code Reporting	(July 2016)
52.204-17	Ownership or Control of Offeror	(July 2016)
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	(Oct 2020)
52.204-26	Covered Telecommunications Equipment or Services-Representation	(Dec 2019)
52.209-7	Information Regarding Responsibility Matters	(Oct 2018)
52.212-3	Offeror Representations and Certifications-Commercial Items	(Nov 2020)
52.212-4	Contract Terms and Conditions-Commercial Items	(Oct 2018)
52.212-5	Contract Terms and Conditions Required to Implement Statues or Executive Orders – Commercial Items	(May 2019)
52.217-8	Option to Extend Services	(Nov 1999)
52.217-9	Option to Extend the Term of the Contract	(Mar 2000)
52.219-9	Small Business Subcontracting Plan	(Sep 2021)
52.223-15	Energy Efficiency in Energy Consuming Products	(Dec 2007)
52.227-14	Rights In Data – General Alternate II and III	(May 2014)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-16	Additional Data Requirements	
52.232-18	Availability of Funds	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-40	Providing Accelerated Payment to Small Business Subcontractors	(Dec 2013)
52.244-6	Subcontracts for Commercial Items	(Jul 2014)
52.251-1	Government Supply Sources	(Apr 2012)

Clause No	Clause Title	Date
52.207-5	Option to Purchase Equipment.	(Feb 1995)
52.243-4	Changes	(Feb 1995)
52.203-6	Restrictions on Subcontractor Sales to the Government	(Sept 2006)
52.249-14	Excusable Delays	(Apr 1984)
52.248-1	Value Engineering	(Oct 2010)
52.204-2	Security Requirements	(Aug 1996)
52.204-9	Personal Identity Verification of Contractor Personnel	(Sept 2007)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.239-1	Privacy or Security Safeguards	(Aug 1996)

8.2 The full text of a provision may be accessed electronically at: GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.232.25	Prompt Payment	(Nov 2009)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)
552.204-9	Personal Identity Verification Requirements	(Oct 2012)
552.236-75	Use of Premises	(Apr 1984)
552.239-70	Information Technology Security Plan and Security Authorization	(Jun 2011)

SECTION 9 – ATTACHMENT LIST

The following are applicable documents for this solicitation:

Attachment A: Quality Assurance Surveillance Plan (QASP)

Attachment B: Past Performance Questionnaire

Attachment C: Conflict of Interest Form

SECTION 10 – INSTRUCTIONS, CONDITIONS, AND NOTICES TO QUOTER

10.1. GENERAL INSTRUCTIONS

The government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the government reserves the right to conduct discussions if later determined by the CO to be necessary. The government contemplates a firm-fixed price contract award for this requirement. Offerors shall submit quotes to the government that clearly

detail proposed technical capabilities to meet the requirements contained within this solicitation. The offeror's proposal shall be clear, concise, and shall include sufficient detail for effective evaluation and for substantiating the validity of stated claims. The proposal shall not simply rephrase or restate the government's requirements, but rather provide convincing rationale to address how the offeror intends to meet these requirements.

10.1.1. Relative Importance of Evaluation Factors.

Regarding the relative importance of each factor: Technical and Past Performance when combined are significantly more important than price. The government reserves the right to award a contract other than to the offeror with the lowest price. However, in the event quotes are evaluated as equal in technical components, price will become a major consideration in selecting the successful.

10.1.2. Discrepancies.

If an offeror believes that the requirements in these instructions contain an error, omission, or are otherwise unsound, the offeror shall immediately notify the CO in writing with supporting rationale as well as the remedies the offeror is asking the CO to consider as related to the omission or error.

10.1.3. Volumes

Offerors submitting a proposal in response to this RFQ shall submit three (3) separate volumes:

- Volume I – Technical Approach
- Volume II – Past Performance
- Volume III – Price

Offerors must ensure that pricing information is only included in **Volume III**. DO NOT include any pricing information in Volume I or Volume II. All unit and extended prices provided shall be rounded to the nearest dollar. Extended prices must be divisible by the number of units proposed. All loaded labor rates shall be rounded to the nearest penny.

10.1.4. Page Limitations

Page limitations shall be treated as maximums. If exceeded, the excess pages will not be read or considered in the evaluation of the proposal. Blank pages, title pages, cover pages, table of contents, tab indexing, glossaries, list of tables and figures, subcontractor consent letter(s), and

resumes are not included in page limitation. Legible tables, charts, graphs and figures may be used to depict organizations, systems and layout, implementation schedules, plans, etc.

10.1.5. Page Size and Format

A page is defined as each face of a sheet of paper containing information. When both sides of a sheet display printed material, it shall be counted as two (2) pages. Page size shall be 8½ x 11 inches. Pages shall be single-spaced and typed, except for displays and the reproduced sections of the solicitation document. The font shall be Times New Roman and no less than 12 points in size. Use at least 1-inch margins on the top and bottom. Pages shall be numbered sequentially by volume. When text is included within displays, it may be no smaller than 8-point, but must be clearly legible without magnification, as determined solely by the CO. The size of these displays shall not exceed the page size as defined above. The page size and format restrictions shall also apply to responses to Proposal Revision, if applicable. These limitations shall apply to the electronic copies of quotes.

10.1.6. Title Page

Each volume must include a title page. The title pages must show:

- Solicitation Number
- SAM Unique Entity Identification (UEI) Number
- Tax Identification Number (TIN)
- Dun & Bradstreet Number (DUNS)
- Complete Business Mailing Address
- Contact Name
- Contact Phone Number
- Contact Fax Number
- Contact Email Address

VOLUME	TITLE	RFQ PAGE REFERENCE	COPIES	MAXIMUM NUMBER OF PAGES
I	Technical Approach - *Technical Approach* - *Quality Control Plan* - *Security Requirements*	4-18, 50,51,53	1	50 for *Technical Approach* and *Quality Control Plan* combined. 25 for the *Security Requirements*
II	Past Performance	50-52	1	Unlimited
III	Price	52,56	1	Unlimited

10.2. VOLUME I: TECHNICAL APPROACH

Technical Approach – Technical approach shall present an outline of technical solutions. At a minimum the plan shall include the following: clear understanding and ability to meet all requirements. Technical skills and solutions to meet requirements outlined in the Sections 2.4 and 2.5. The technical approach shall not merely restate the government's objective.

Quality Control – The offeror shall submit its quality control plan as part of their implementation and configuration approach for the performance of contract, including, but not limited to, the firm's quality control program, internal training policies and programs, and specific measures to be enacted for this contract.

Security Requirements – The offeror shall submit a security control plan that meets or exceeds the security requirements referenced in Section 7. Specifically, the security control plan shall identify key personnel, equipment, technologies, and business processes that will be utilized to ensure that the GSA OIG's personnel, operational, and technical security requirements are met.

10.3. VOLUME II: PAST PERFORMANCE

The offeror shall provide proof of a satisfactory record of performance, integrity, and business ethics. The offeror shall provide no less than three (3) and no more than five (5) relevant contracts for the past three (3) years, describing how the work performed relates to GSA OIG requirements for the last three (3) years from the date of issuance of this solicitation. Offerors shall submit information on contracts deemed relevant in demonstrating the ability to perform the full range of capabilities for requirements outlined in the solicitation. Each offeror's proposal

shall provide examples of past performance that indicates a high expectation that the offeror will successfully perform the required effort.

The offeror shall furnish the following information for each past performance reference submitted:

- Company/Division Name
- Description of service and a detailed explanation of relevance to this requirement
- Contracting Agency/Customer point of contact or reference having knowledge of contract performance
- Contract number
- Contract type and dollar value (per year cost and life cycle cost)
- Total number of Full-Time Equivalent FTEs
- Designation as a prime or subcontractor
- Period of Performance
- Completion date
- Verified, up-to-date name, address, and telephone number of the CO
- Comments regarding compliance with contract terms and conditions
- Comments regarding any known performance deemed unacceptable to the customer, or not in accordance with the contract terms and conditions
- Questionnaire log to include the name, address, telephone number, and email address for each point of contact to whom the Past Performance Questionnaire was sent for completion

Offerors are cautioned to ensure respective past performance information submitted is RECENT from the date of issuance of the solicitation. Any past performance information submitted over the maximum of five (5) contracts may be disregarded in its entirety.

Past Performance Questionnaires: Past Performance Questionnaires (Attachment B) shall be sent to the offeror's points of contact. The offeror should make its best effort to provide a sufficient number of past performance questionnaires to reasonably expect the CO will receive at least one (1) response. The offeror is responsible to ensure that the POC information provided is accurate. Questionnaires shall be sent as part of the technical quote electronically to Emmanuel Osei Darko-emmanuel.oseidarko@gsaig.gov.

Teaming Arrangement: If a teaming arrangement is contemplated, provide a summary as to the overall arrangement, including any relevant and recent past performance information on previous teaming arrangements with the same partner. The teaming arrangement summary shall be included in **Volume II – Past Performance**.

10.4. VOLUME III: PRICE

This section is to assist offerors in submitting data other than certified cost or pricing data that is required to evaluate whether prices proposed are fair, reasonable, complete, and balanced. Quotes should be sufficiently detailed to demonstrate their fairness, reasonableness, and balance. The burden of proof for credibility of proposed prices rests with the offeror.

Base Year: October 1, 2023 – September 30, 2023
1st Option: October 1, 2024 – September 30, 2025
2nd Option: October 1, 2025 – September 30, 2026
3rd Option: October 1, 2026 – September 30, 2027
4th Option: October 1, 2027 – September 30, 2028

10.5. SUBMITTING QUOTES

Questions are due eletrononically to emmanuel.oseidarko@gsaig.gov by July 8, 2023, 10:00 AM EST.
Submit your quotes electronically (via email) to Emmanuel Osei Darko at emmanuel.oseidarko@gsaig.gov by July 19, 2023, 3:00 PM EST. All electronic submissions shall reference the complete solicitation number in the subject line.

SECTION 11 – EVALUATION FACTORS FOR AWARD

11.1. EVALUATION PROCESS

The government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the government, price and other factors considered, and conforms to this Request for Quotation terms and conditions. Tradeoffs will be made between Past Performance and Price among those offerors who have been determined to be technically acceptable. Non-price factors (Technical and Past Performance when combined) are significantly more important than price.

11.2. EVALUATION STEPS

The following evaluation steps will be followed:

11.2.1. Step 1: Quotation Adequacy

The government will review quotes for conformity and completeness (adhering to all information/instructions in the Instruction to Offerors). If an offeror fails to comply with instruction in Section 10, the offeror's quote may be deemed nonresponsive and/or incomplete and will receive no further consideration and be eliminated from the competition. The government will only further evaluate quotes deemed responsive and complete. Note: The government will not search for data to cure problems or address inconsistencies in an offeror's quotes.

11.2.2. Step 2: Technical Approach Evaluation

The technical evaluation includes an evaluation of the offeror's quote.

- Technical Factor 1: Requirements. This factor involves evaluating the software's capabilities against the Software Requirements sections of the SOW.
- Technical Factor 2: Implementation and Configuration Requirements. This factor involves evaluating how thoroughly the offeror explains and outlines their plans for the Implementation and Configuration Requirements of the SOW.
- Technical Factor 3: A review of each offeror's Security Requirements and Quality Control Plan

11.2.3. Step 3: Past Performance Evaluation

The government will evaluate past performance. The government will evaluate the offeror's past performance submissions for recency, relevancy, and quality to determine an overall Past Performance Confidence Assessment rating. The CO may determine to eliminate any quote receiving a low overall confidence rating from further consideration.

A copy of the Past Performance Questionnaire is included in the RFQ as an attachment and addresses key success factors of how past performance will be evaluated. Specific elements provided in the survey that are considered important to the evaluation include:

- Quality of services provided
- Timeliness of products in meeting contract requirements and milestones
- Accuracy and completeness of invoices submitted for payment
- Staff qualifications of personnel assigned to the contract

Offeror should consider subcontractor past performance submission if their quote includes substantial subcontracting efforts.

11.2.3.1. Recency Assessment

A recency determination will be made for each contract reference provided. To be recent, the effort shall exhibit continuous active contract performance and the software should have at least 3 years of audit or inspection usage. Past performance information that fails this condition will not be evaluated.

11.2.3.2. Relevancy Assessment

A relevancy determination will be made for each individual past performance submission. The government is not bound by the offeror's opinion of relevancy. Equal consideration will be given to the effort being proposed by the offeror, teaming partner, or subcontractor whose contract is being reviewed and evaluated.

11.2.3.3. Quality Assessment

The government evaluation team will conduct an in-depth review and evaluation of all recent and relevant past performance and will determine the quality and usefulness as it applies to the Past Performance Confidence rating.

11.2.3.4. Confidence Rating

The government will consider past performance in the aggregate when forming a confidence rating. The government evaluation team will consider the offeror's past performance as an entire team (where primes propose with subcontractors) or on an individual basis for contractors proposing on their own.

Individual contract past performance regarding predecessor companies or subcontractors that will perform major or critical aspects of the requirement will be rated the same as past performance information for the principal offeror; however, offerors with relevant past performance as a prime contractor may be assessed a higher rating than offerors without any relevant past performance as a prime contractor.

Offerors with no recent/relevant performance history or if the offeror's performance record is so sparse that no meaningful rating can be reasonably made will be treated neutrally, meaning the rating is neither favorable nor unfavorable. However, since the government has stated that technical approach when combined with past performance receives greater consideration than price, a strong record of relevant past performance may be considered more advantageous to the government than a neutral past performance rating.

In addition to surveys. past performance information may be obtained through one or more of the following:

- Past Performance Information Retrieval System (PPIRS)
- Contract Performance Assessment Reporting System (CPARS)
- Federal Awardee Performance and Integrity Information System (FAPIIS)
- Electronic Subcontract Reporting System (eSRS)
- Questionnaires tailored to the circumstances of this acquisition or other sources or databases known to the government
- Interviews may be conducted with program managers, contracting officers, fee determining officials and the defense contract management agency or other sources known to the government

11.2.4. Step 4: Price

The total evaluated price, base period and all option periods, will be evaluated for fairness, reasonableness, completeness, and balance. Only quotes determined to be fair, reasonable, complete, and balanced will be considered for award. This RFQ contains FAR Clause 52.217-8, Option to Extend Services. This option period will be evaluated as part of initial competition. Evaluation of options will not obligate the government to exercise the option(s).

The Total Evaluated Price (TEP) will consist of the sum of the fully burdened firm-fixed price (FFP) CLINs.

11.2.4.1. Price

The government will evaluate the reasonableness of proposed price. For the price to be reasonable in its nature and amount, it should not exceed that which would be incurred by a prudent person in the conduct of a competitive business. An offer that is determined to be unreasonably high will not be considered for award.

11.2.4.2. Unbalanced Pricing

Offerors are cautioned against submitting an offer that contains unbalanced pricing. Unbalanced pricing may increase performance risk and could result in payment of unreasonably high prices. Unbalanced pricing exists when, despite an acceptable total evaluated price, the price of one (1) or more contract line items is significantly over or understated. An offer that is determined to be unbalanced may be rejected if the CO determines that the lack of balance poses an unacceptable risk to the government.