



U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer • Employee Benefits Security Administration

Employee Benefits Security Administration's (EBSA) – Employee Retirement Income Security Act of 1974 (ERISA) Filing Acceptance System II (EFAST2) Rebuild/Modernization

VOLUME I

Technical Approach

Factor I — Technical Capability

Solicitation No.	1605TA-26-Q-00055
Issuing agency	U.S. Department of Labor — OCIO / EBSA
NAICS / size standard	541512 — Computer Systems Design Services / \$34M
Set-aside	100% Small Business
Contract type	Firm-Fixed-Price Task Order
Quotation due	September 14, 2026 at 12:00 P.M. ET

PREPARED FOR AND PRESENTED TO

U.S. Department of Labor

Office of the Senior Procurement Executive (OSPE)
Information Technology Acquisition Services
200 Constitution Avenue, NW, Room S-4307
Washington, DC 20210

Nicole D. Jacobs, Contracting Officer

Jacobs.Nicole.D@dol.gov

Jackia S. Barnes, Contract Specialist

Barnes.Jackia.S@dol.gov • (202) 693-4148

PREPARED AND PRESENTED BY

[Company Name]

[Street Address] • [City, State ZIP]

[Insert Company Logo]

[Name], [Title]

[Email Address] • [Phone Number]

UEI [UEI] • CAGE [CAGE]

GSA MAS No. [Number] • SIN 54151S

[Socio-Economic Status per SAM.gov]

USE OR DISCLOSURE OF DATA — RESTRICTIVE LEGEND

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained on the pages marked with the legend "Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal."

Cover Letter

PLACEMENT NOTE.

The RFQ states that the AI Use Disclosure responses "are excluded from the volume page limits" and "must be placed behind the cover letter preceding Volume 1" (Instructions C and G). The cover letter and the AI Use Disclosure have been placed here, ahead of the Table of Contents, at the direction of the proposal team. They are submittable content, not outline scaffolding: do not delete them. Delete only the coloured boxes and the red notices.

The cover letter is limited to two pages and the AI Use Disclosure to one page. Neither counts against the 45-page Volume I limit.

INSTRUCTIONS (Instructions to Vendors, G. Cover Letter):

G. Cover Letter *The cover letter is considered the first page of the Quotation and must include the following:*

- Statement that the quote is firm for a period of not less than 120 calendar days from the quote due date.
- Statement of compliance indicating either complete compliance with the solicitation or a detailed analysis of any objections, exceptions, or contingencies to the terms of the solicitation.
- Statement regarding the vendor's compliance with RFO FAR 9.104-1 (General Standards for Responsible Prospective Contractors).
- Complete business address of the vendor, the corporate name to be used on any resultant contract, and the remittance address if different from above. If this name does not identify a "parent company" or sponsoring "corporation" name, also provide such identity, as appropriate and the vendor's SAM unique entity identifier (UEI) code.
- Socio Economic Status (as registered in SAM.gov).
- Solicitation Number.
- GSA Multiple Award Schedule (MAS) Contract Number and applicable SIN(s)
- No more than two points of contact information to include name, phone numbers and email address(es).
- Submission for AI Disclosure responses are excluded from the volume page limits. However, responses to this information are limited to one page and must be placed behind the cover letter preceding Volume 1.

Instructions G, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 155

PAGE LIMIT: Cover letter not to exceed (NTE) 2 pages (Instructions C). EXCLUDED FROM PAGE LIMIT: the cover letter is not part of the Volume I 45-page count (Instructions C).

[Company Letterhead — insert logo, address and contact line]

September 14, 2026

Volume I - Technical Approach

Ms. Nicole D. Jacobs

Contracting Officer

U.S. Department of Labor

Office of the Senior Procurement Executive (OSPE)

Information Technology Acquisition Services

200 Constitution Avenue, NW, Room S-4307

Washington, DC 20210

cc: Ms. Jackia S. Barnes, Contract Specialist — Barnes.Jackia.S@dol.gov — (202) 693-4148

Subject: RFQ No. 1605TA-26-Q-00055 — Employee Benefits Security Administration's (EBSA) Employee Retirement Income Security Act of 1974 (ERISA) Filing Acceptance System II (EFAST2) Rebuild/Modernization Quotation Submission — Volume I: Technical Approach

Dear Ms. Jacobs:

Transmittal. [Company Name] is pleased to submit this quotation in response to Request for Quotation (RFQ) No. 1605TA-26-Q-00055 for the EFAST2 Rebuild/Modernization requirement, issued by the U.S. Department of Labor on behalf of the Office of the Chief Information Officer (OCIO) and the Employee Benefits Security Administration (EBSA). Our quotation is submitted in three separate volumes — Volume I: Technical Approach, Volume II: Management Approach, and Volume III: Price — together with the completed Attachment #1 (Price Schedule) and Attachment #2 (Payment Schedule) in Microsoft Excel format. The one-page AI Use Disclosure required by DOL 2026-01 is placed immediately behind this letter and preceding Volume I. This letter constitutes the first page of the quotation.

Quotation validity. [Company Name] confirms that this quotation is firm and irrevocable for a period of not less than 120 calendar days from the quotation due date of September 14, 2026, and may be accepted by the Government at any time within that period without further action by the Quoter.

Statement of compliance. [Select one and delete the other.] [Option A — full compliance:] [Company Name] takes no exception to the terms, conditions, instructions, evaluation criteria, Performance Work Statement, Technical Exhibits, attachments, clauses, or any other provision of RFQ No. 1605TA-26-Q-00055, and is in complete compliance with the solicitation as issued and as amended. [Option B — exceptions taken:] [Company Name] is in compliance with the solicitation with the following exceptions: [state each objection, exception, or contingency; cite the specific RFQ page, section and paragraph; explain the basis; and state the proposed alternative language and its effect on price, schedule and risk]. Our quotation is not conditional and does not make award contingent upon acceptance of any exception.

Responsible prospective contractor — RFO FAR 9.104-1. [Company Name] represents that it meets each of the general standards for responsible prospective contractors set out at RFO FAR 9.104-1. Specifically, the firm has adequate financial resources to perform this task order or

Volume I - Technical Approach

the ability to obtain them; is able to comply with the required and proposed delivery and performance schedule, taking into consideration all existing commercial and governmental business commitments; has a satisfactory performance record; has a satisfactory record of integrity and business ethics; has the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them; has the necessary production, construction and technical equipment and facilities, or the ability to obtain them; and is otherwise qualified and eligible to receive an award under applicable laws and regulations. [Insert two to three sentences of substantiation — for example, audited financial capacity, current CPARS or reference ratings, ISO/CMMI or equivalent process certifications, and active, unexcluded registration in SAM.gov.]

Understanding and commitment. [Insert three to five sentences. State the Quoter's understanding that EFAST2 accepts and publicly discloses ERISA annual return/report filings on a fixed statutory cycle; commit to assuming full contractual responsibility within thirty (30) calendar days of award with minimal Government involvement in knowledge transition; commit to delivering the January 1 annual rollover release on schedule; and commit to performing without disruption or degradation to filer services, Contact Center operations, or the continuity of legacy data back to 2009. Keep this paragraph substantive and specific — general or vague statements are expressly identified in the RFQ as an indication of a lack of understanding.]

Quoter identification. The corporate and registration information required by Instructions, paragraph G, is provided in Exhibit 1-1 below. All information reflects the Quoter's active registration in the System for Award Management (www.sam.gov) as of the date of this letter.

Required element (Instructions, G)	Quoter response
Corporate name to be used on any resultant contract	[Legal entity name exactly as registered in SAM.gov]
Parent company or sponsoring corporation	[Name, or "Not applicable — [Company Name] is not a subsidiary"]
Complete business address	[Street Address; City, State ZIP]
Remittance address (if different from above)	[Street Address; City, State ZIP, or "Same as business address"]
Unique Entity Identifier (UEI), SAM.gov	[12-character UEI]
CAGE Code	[5-character CAGE]
Socio-economic status (as registered in SAM.gov)	[e.g., Small Business; SDVOSB; 8(a); HUBZone; WOSB — list all that apply]
SAM.gov registration status	Active and unexcluded as of [date]; registration expires [date]
Solicitation number	1605TA-26-Q-00055
NAICS code and size standard	541512 — Computer Systems Design Services; \$34M (100% small business set-aside)
GSA Multiple Award Schedule (MAS) contract number	[GS-XXX-XXXXXX / 47QTCA-XX-D-XXXX]

Required element (Instructions, G)	Quoter response
Applicable Special Item Number(s) — SIN(s)	[e.g., 54151S Information Technology Professional Services; list every SIN used]

Exhibit 1-1. Quoter Identification (Inst. G)

Points of contact. In accordance with Instructions, paragraph G, no more than two points of contact are designated for this quotation. Primary: [Name], [Title], [Phone Number], [Email Address]. Alternate: [Name], [Title], [Phone Number], [Email Address]. Either individual is authorized to respond to Government questions regarding this quotation and to receive notices under RFQ No. 1605TA-26-Q-00055.

AI Use Disclosure. In accordance with DOL 2026-01, Artificial Intelligence (AI) in IT Requirements (April 2026), [Company Name]’s AI Use Disclosure is provided on the single page immediately following this letter and preceding Volume I. That response is limited to one page and, per the RFQ page-count table, is excluded from the volume page limits.

Closing. [Company Name] appreciates the opportunity to quote on this requirement and is prepared to begin performance immediately upon award. Questions regarding this quotation may be directed to the primary point of contact identified above.

Sincerely,

[Authorized Signatory Full Name]
[Title]
[Company Name]
[Email Address] | [Phone Number]
Date: [Date]

AI Use Disclosure

PAGE LIMIT: Limited to one page (Instructions C). EXCLUDED FROM PAGE LIMIT: AI Use Disclosure responses are excluded from the volume page limits and must be placed behind the cover letter preceding Volume 1 (Instructions C, Instructions G).

RFQ CLAUSES (DOL 2026-01, Disclosure of AI Use):

Disclosure of AI Use

- The contractor must disclose whether AI was used to write the proposal/quotation or any other section in its response to the solicitation.
- The contractor must provide a brief description of how AI tools were utilized in the process of developing the proposal/quotation, including the types of tasks performed by AI (e.g., data analysis, content generation, document review).
- The contractor must disclose to the Government any intended or incidental use of AI in the performance of this PWS. This includes AI used in internal processes or tools that may influence contract deliverables, even if not explicitly required by the Government.
- The contractor must provide a statement affirming that all AI-generated content has been subjected to review by qualified personnel to ensure accuracy, relevance, and compliance with solicitation requirements.

DOL 2026-01, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 135

RFQ CLAUSES (DOL 2026-01, Approval and Tracking):

Approval and Tracking

- ***Contractors that intend to use AI tools and systems in performance of a contract action and/or produce contract deliverables must disclose the use of such tools as part of its proposal/quotation.*** Contractors using AI tools and systems to perform under an awarded contract action must identify the product being used and submit that tool for agency approval.
- Contractors must implement the applicable system security controls as detailed in the Security and Privacy section of the Performance Work Statement (PWS) for any AI tools or system used to support DOL work that is located outside of DOL.
- Contractors are to assist the agency in identifying reasonably foreseeable use cases arising from the use of AI tools, systems, or services likely to host high-impact AI use cases.

DOL 2026-01, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 132

THIS DISCLOSURE IS REQUIRED EVEN IF NO AI WAS USED.

The clause requires the contractor to disclose "whether AI was used" to write the quotation. A negative

Volume I - Technical Approach

statement is still a required submission. Answer all four bullets of the Disclosure of AI Use clause explicitly.

Required element	RFQ requirement, verbatim, and what to write
1. Whether AI was used to write the quotation	The contractor must disclose whether AI was used to write the proposal/quotation or any other section in its response to the solicitation. What the letter must say: <i>[State plainly whether AI was used to write the quotation or any other section of the response to this solicitation. A negative statement is still a required submission: the clause requires disclosure of whether AI was used, so answer even if the answer is no.]</i>
2. How AI tools were used	The contractor must provide a brief description of how AI tools were utilized in the process of developing the proposal/quotation, including the types of tasks performed by AI (e.g., data analysis, content generation, document review). What the letter must say: <i>[Provide a brief description of how AI tools were used in developing the quotation, including the types of tasks performed by AI. The clause names three examples: data analysis, content generation and document review. If no AI was used, state that this bullet is not applicable and say why.]</i>
3. Intended or incidental AI use in performance of the PWS	The contractor must disclose to the Government any intended or incidental use of AI in the performance of this PWS. This includes AI used in internal processes or tools that may influence contract deliverables, even if not explicitly required by the Government. What the letter must say: <i>[Disclose any intended or incidental use of AI in performing this PWS, including AI used in internal processes or tools that may influence contract deliverables even where the Government does not require it. PWS 5.4.5 and PWS 5.8.2 contemplate AI-enabled development and a chatbot solution, so this bullet will normally be answered in the affirmative.]</i>
4. Qualified-personnel review affirmation	The contractor must provide a statement affirming that all AI-generated content has been subjected to review by qualified personnel to ensure accuracy, relevance, and compliance with solicitation requirements. What the letter must say: <i>[Provide a statement affirming that all AI-generated content has been reviewed by qualified personnel for accuracy, relevance and compliance with solicitation requirements. Name the role that performed the review.]</i>
5. AI product identification and agency approval	Contractors that intend to use AI tools and systems in performance of a contract action and/or produce contract deliverables must disclose the use of such tools as part of its proposal/quotation. Contractors using AI tools and systems to perform under an awarded contract action must identify the product being used and submit

Volume I - Technical Approach

Required element	RFQ requirement, verbatim, and what to write
	that tool for agency approval. What the letter must say: <i>[If [Company Name] intends to use AI tools or systems in performance of the contract action or to produce contract deliverables, disclose that use here and identify the product. The same bullet requires the tool to be submitted for agency approval after award.]</i>

Exhibit 1-2. AI Use Disclosure Required Elements (DOL 2026-01)

Cross-Reference Matrix

INSTRUCTIONS (Instructions to Vendors, E. Glossary and Acronyms):

For clarity and completeness of presentation, *vendors must provide a cross-reference matrix for each of the volumes listed*. This matrix must be placed after the cover page for each volume, and must indicate the quotation volume section, subsection, and paragraph, cross-referenced with the appropriate PWS paragraphs, applicable RFQ instructions, evaluation criteria, and task order deliverables, as applicable.

Instructions E, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 154-155

CROSS-REFERENCE MATRIX IS NOT EXCLUDED FROM THE 45-PAGE LIMIT.

Instructions E requires the matrix and fixes its position: "This matrix must be placed after the cover page for each volume." No exclusion clause in the RFQ removes it from the page count. Budget pages for it, or ask the Contracting Officer to confirm the treatment before the question deadline.

The matrix is placed here, at the end of the front matter, so that it follows the cover page and the Table of Contents. Move it if the Contracting Officer directs otherwise.

Volume Section, Subsection and Paragraph	PWS Paragraph	Applicable RFQ Instruction	Evaluation Criterion	Task Order Deliverable
[Insert outline section number and heading]	[Insert PWS paragraph]	[Insert Instructions reference]	[Insert Evaluation reference]	[Insert TE2 deliverable number, or N/A]
[Insert outline section number and heading]	[Insert PWS paragraph]	[Insert Instructions reference]	[Insert Evaluation reference]	[Insert TE2 deliverable number, or N/A]
[Insert outline section number and heading]	[Insert PWS paragraph]	[Insert Instructions reference]	[Insert Evaluation reference]	[Insert TE2 deliverable number, or N/A]

Exhibit 1-3. Cross-Reference Matrix (Inst. E)

Add one row for every section, subsection and paragraph of this volume. The four right-hand columns are the four cross-references Instructions E names.

Table of Contents

VOLUME I - TECHNICAL APPROACH	1
1 UNDERSTANDING OF THE EFAST2 REBUILD/MODERNIZATION REQUIREMENT (INST. VOL I)	1
1.1 UNDERSTANDING OF THE OBJECTIVES (PWS 1.3)	2
1.2 UNDERSTANDING OF THE SCOPE (PWS 1.4)	4
1.3 UNDERSTANDING OF THE PERFORMANCE REQUIREMENTS SUMMARY (TE 1)	5
1.4 UNDERSTANDING OF THE DELIVERABLES SCHEDULE (TE 2)	5
1.5 UNDERSTANDING OF THE DELIVERABLE ACCEPTANCE PROCEDURES (TE 2)	6
2 TECHNICAL APPROACH, METHODS, DEVELOPMENT PRACTICES, AND TOOLS (INST. VOL I)	8
2.1 TRANSITION-IN AND ASSUMPTION OF FULL CONTRACTUAL RESPONSIBILITY WITHIN THIRTY DAYS OF AWARD (PWS 5.1, INST. VOL I)	9
2.2 PROJECT MANAGEMENT SERVICES AND IMPLEMENTATION OF AGILE PRACTICES AT DOL (PWS 5.2, INST. VOL I)	11
2.2.1 Monthly Progress Report (MPR) (PWS 5.2.1)	14
2.2.2 Weekly Progress Report (WPR) (PWS 5.2.2)	14
2.3 DESIGN & PROTOTYPE DEVELOPMENT (PWS 5.3)	14
2.4 DESIGN & DEVELOPMENT (PWS 5.4)	15
2.4.1 Registration Portal (PWS 5.4.1)	16
2.4.2 Filing Acceptance Service (PWS 5.4.2)	17
2.4.2.1 Filing Submission Flow (PWS 5.4.2.1)	17
2.4.2.2 Filer Authentication (PWS 5.4.2.2)	18
2.4.3 Third-Party Software Support (PWS 5.4.3)	19
2.4.3.1 Third-Party Software Certification Criteria (PWS 5.4.3.1)	20
2.4.3.2 Filing Preparation Software Test Scenarios (PWS 5.4.3.2)	20
2.4.3.3 Transmission Software (PWS 5.4.2.3)	21
2.4.3.4 Third-Party Software Authorization (PWS 5.4.3.4)	22
2.4.3.5 Third-Party Software Developer Conference (PWS 5.4.3.5)	22
2.4.3.6 Guide for Filers and Service Providers (PWS 5.4.3.6)	22
2.4.3.7 Software Developer's Specification (PWS 5.4.3.7)	23
2.4.3.8 Participant Acceptance Testing System (PATs) Test/Certification Program (PWS 5.4.3.8)	23
2.4.3.9 PATs Test Filings (PWS 5.4.3.9)	24
2.4.3.10 Third-Party Software Test Plan and Certification Procedures (PWS 5.4.3.10)	24
2.4.3.11 Annual Updates and Certifications (PWS 5.4.3.11)	25
2.4.3.12 Software Developer Monitoring (PWS 5.4.3.12)	25
2.4.4 Filing Guidelines (PWS 5.4.4)	25
2.4.4.1 Unauthenticated User Applications (PWS 5.4.4.1)	26
2.4.4.2 PII Review of Flagged Attachments (PWS 5.4.4.2)	26
2.4.4.3 Public Disclosure After PII Review (PWS 5.4.4.3)	27
2.4.4.4 Revoke Public Access and Disclosure Changes (PWS 5.4.4.4)	27
2.4.4.5 Authenticated Filer Applications (PWS 5.4.4.5)	28

Volume I - Technical Approach

2.4.4.6	My Filings (PWS 5.4.4.6)	28
2.4.4.7	Filing Web Application (PWS 5.4.4.7)	29
2.4.4.7.1	Filing Creation (PWS 5.4.4.7.1)	29
2.4.4.7.2	Filing Signing (PWS 5.4.4.7.2)	31
2.4.4.7.3	Filing Submission (PWS 5.4.4.7.3)	32
2.4.4.7.4	Form PR (PWS 5.4.4.7.4)	32
2.4.4.7.5	Authenticated Government Functions (PWS 5.4.4.7.5)	33
2.4.5	<i>Artificial Intelligence (AI)-Enabled Development, Modernization, and Enhancement (DME) (PWS 5.4.5)</i>	34
2.4.5.1	Proactive use of AI (PWS 5.4.5.1)	34
2.4.5.2	Transparency and prior notification (PWS 5.4.5.2)	35
2.4.5.3	Security, privacy, and data handling (PWS 5.4.5.3)	35
2.4.5.4	Quality and compliance (PWS 5.4.5.5)	36
2.4.5.5	Intellectual property and deliverables (PWS 5.4.5.6)	36
2.5	DIRECT USER EXCHANGE (PWS 5.5)	37
2.5.1	<i>Website (PWS 5.5.1)</i>	37
2.5.2	<i>Compatibility and Accessibility (PWS 5.5.2)</i>	39
2.5.3	<i>Cookies and Session Data (PWS 5.5.3)</i>	40
2.6	DATA DISSEMINATION (PWS 5.6)	40
2.7	REPORTS (PWS 5.7)	40
2.8	CONTACT CENTER (PWS 5.8)	41
2.8.1	<i>Written Inquiries (PWS 5.8.1)</i>	42
2.8.2	<i>Chatbot/AI Solution (PWS 5.8.2)</i>	43
2.8.3	<i>Release Notes (PWS 5.8.3)</i>	45
2.9	DATA MANAGEMENT AND MIGRATION (PWS 5.9)	45
2.10	TESTING AND DEPLOYMENT (PWS 5.10)	46
2.11	DEVSECOPS (PWS 5.11)	47
2.12	RELEASE MANAGEMENT (PWS 5.12)	48
2.13	OPERATIONS AND MAINTENANCE (O&M) (PWS 5.13)	49
2.13.1	<i>Operations (PWS 5.13.1)</i>	50
2.13.2	<i>Maintenance and Release/Change Management (PWS 5.13.2)</i>	50
2.13.3	<i>Security, Privacy, and Compliance (Continuous ATO) (PWS 5.13.3)</i>	51
2.13.4	<i>Monitoring, Incident, and Problem Management (PWS 5.13.4)</i>	51
2.13.5	<i>Data Management, Backup, and Continuity (PWS 5.13.5)</i>	52
2.13.6	<i>Environment Stewardship and Tools (PWS 5.13.6)</i>	52
2.13.7	<i>Annual Forms Changes (PWS 5.13.7)</i>	53
2.13.7.1	Annual Forms, Schedules, and Instructions Development (PWS 5.13.7.1)	53
2.13.7.2	Annual Rollover Requirement Development (PWS 5.13.7.2)	54
2.13.7.3	Annual Rollover Updates (PWS 5.13.7.3)	55
2.13.7.4	Annual System Maintenance Rollover Changes (PWS 5.13.7.3)	56
2.13.8	<i>System Architecture (PWS 5.13.8)</i>	57
2.13.8.1	Availability (PWS 5.13.8.1)	57
2.13.8.2	Scaling (PWS 5.13.8.2)	58
2.13.8.3	Disaster Recovery (PWS 5.13.8.3)	58
2.13.8.4	Backups (PWS 5.13.8.4)	59

Volume I - Technical Approach

2.13.8.5	Service Level Agreement (PWS 5.13.8.5)	59
2.13.8.6	Detailed System Design (PWS 5.13.8.6)	59
2.13.8.7	System Sizing Analysis (PWS 5.13.8.7)	60
2.13.8.8	Benchmark Report (PWS 5.13.8.8)	60
2.13.8.9	System Performance Report (PWS 5.13.8.9)	61
2.13.8.10	Asset and Supplier Inventory (PWS 5.13.8.10)	62
2.13.8.11	Data Archival Support (PWS 5.13.8.11)	62
2.14	TRANSITION-OUT (PWS 5.14)	62
3	FUNCTIONAL, SECURITY, AND COMPLIANCE REQUIREMENTS (INST. VOL I)	65
3.1	FEDRAMP (PWS 1.4)	66
3.2	FISMA AND NIST SP 800-53 REV. 5 (TE 3)	67
3.3	IRS PUBLICATION 1075 (PWS 6.1.2)	68
3.4	IDENTITY MANAGEMENT AND AUTHENTICATION (PWS 5.4.2.2)	69
3.5	SECTION 508 AND WCAG 2.1 A/AA ACCESSIBILITY (TE 4)	70
3.6	PHYSICAL SECURITY (PWS 1.6.8.1)	71
3.7	CONSERVATION OF UTILITIES (PWS 1.6.8.2)	71
3.8	APPLICABLE PUBLICATIONS (PWS 6.1)	71
3.9	CLEARANCE (PWS 4.2)	73
4	KEY RISKS AND CREDIBLE MITIGATION STRATEGIES (INST. VOL I)	73
5	RELEVANT EXPERIENCE AND FAMILIARITY WITH LARGE-SCALE FEDERAL IT MODERNIZATION (INST. VOL I)	75
5.1	LARGE-SCALE FEDERAL IT MODERNIZATION (EVALUATION FACTOR I)	76
5.2	ELECTRONIC FILING OR DATA COLLECTION SYSTEMS (EVALUATION FACTOR I)	76
5.3	CLOUD-BASED FEDERAL ENVIRONMENTS (EVALUATION FACTOR I)	77
5.4	THIRD-PARTY SOFTWARE SUPPORT AND CERTIFICATION PROGRAMS (EVALUATION FACTOR I)	77
5.5	CONTACT CENTER OPERATIONS (EVALUATION FACTOR I)	77
5.6	AGILE SOFTWARE DEVELOPMENT (EVALUATION FACTOR I)	78

List of Exhibits

Exhibit 1-1. Example of Table with Dark Heading Row (Caption Style)	
Exhibit 1-2. Example of Table with Dark Heading and Shaded Rows (Caption Style)	
Exhibit 1-3. Example of Table with No Heading Row (Caption Style)	
Exhibit 1-4. Example of Table with No Heading but Shaded Rows (Caption Style)	
Exhibit 1-5. Caption Style (Set graphics to: Layout, In line with text)	

Glossary of Abbreviations and Acronyms

INSTRUCTIONS (Instructions to Vendors, E. Glossary and Acronyms):

E. Glossary and Acronyms *A glossary of acronyms and terms for each volume must be provided* which (including table of contents) will not count against the volume page limit. All acronyms must be defined at first use.

Instructions E, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 154

CROSS-REFERENCE MATRIX IS NOT EXCLUDED FROM THE 45-PAGE LIMIT.

Instructions E requires the matrix and fixes its position: "This matrix must be placed after the cover page for each volume." No exclusion clause in the RFQ removes it from the page count. Against a forty-five volume that is material. Ask the Contracting Officer to confirm the treatment before the question deadline.

Abbreviation/Acronym	Definition
AAL	Authenticator Assurance Levels
AAL2	Not defined in provided RFQ documents. Define at first use per Instructions E.
AES	The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.
API	Not defined in provided RFQ documents. Define at first use per Instructions E.
AQL	Acceptable Quality Level
ATO	Authority to Operate
AWS	Amazon Web Services
BAS	Business Applications Services
BOM	Not defined in provided RFQ documents. Define at first use per Instructions E.
CAGE	Not defined in provided RFQ documents. Define at first use per Instructions E.
CAIO	Chief Artificial Intelligence Officer
CAP	Contractor-Acquired-Government Owned Property
CAT	Customer Acceptance Test. The EFAST2 environment utilized by the Government to conduct systems acceptance testing prior to release to production.
CDR	Contract Discrepancy Report

Volume I - Technical Approach

Abbreviation/Acronym	Definition
CFR	Not defined in provided RFQ documents. Define at first use per Instructions E.
CI/CD	Not defined in provided RFQ documents. Define at first use per Instructions E.
CISA	Not defined in provided RFQ documents. Define at first use per Instructions E.
CISO	Chief Information Security Officer
CISSP	Computer Information Systems Security Professional Certification.
CLIN	Contract Line Item Number. Individual items or components of a multiple item contract can be identified with a Contract Line Item Number.
COR	Contracting Officer Representative
COTS	Commercial-off-the-Shelf Software. Turn-key system, possibly something you could find already available in a store.
CPP	Cybersecurity Policy Portfolio
CRM	Not defined in provided RFQ documents. Define at first use per Instructions E.
CTA	Contractor Teaming Arrangement
CUI	Controlled Unclassified Information. Designation for information that requires safeguarding or dissemination controls. This designation was created under Executive Order 13556 and includes information formerly designated by such markings as For Official Use Only and Sensitive But Unclassified.
DAST	Not defined in provided RFQ documents. Define at first use per Instructions E.
DBA	Not defined in provided RFQ documents. Define at first use per Instructions E.
DEI	Diversity, equity, and inclusion
DER	Data Elements Requirements Document. The governing technical document and associated XML Schema files which dictate the requirements for the data elements and edit test logic applicable to EFAST2.
DEV	Not defined in provided RFQ documents. Define at first use per Instructions E.
DevSecOps	A security focused, continuous delivery, software development life cycle practice.
DFE	Direct Filing Entity. A master trust investment account, common/collective trust, pooled separated account, 103-12 investment entity, or group insurance arrangement.
DME	Modernization Development, Modernization, and Enhancement
DNS	Not defined in provided RFQ documents. Define at first use per Instructions

Volume I - Technical Approach

Abbreviation/Acronym	Definition
	E.
DOL	Department of Labor
DOLAR	Not defined in provided RFQ documents. Define at first use per Instructions E.
DSD	Detailed System Design
EBSA	Employee Benefits Security Administration is an agency within DOL.
EFAST2	ERISA Filing Acceptance System II. EFAST2 is a system designed to simplify and expedite the receipt and processing of the Form 5500 series.
EIN	Employer Identification Number. A unique number assigned by the Internal Revenue Service to every employer in the United States for the purposes of identification.
EIT	Electronic and Information Technology
eQIP	Not defined in provided RFQ documents. Define at first use per Instructions E.
ERISA	Employee Retirement Income Security Act of 1974
ETL	Extract, Transform, and Load
FAQ	Not defined in provided RFQ documents. Define at first use per Instructions E.
FAR	Federal Acquisition Regulation
FedRAMP	The Federal Risk and Authorization Management Program
FFP	firm fixed price
FIPS	Federal Information Processing Standards.
FISMA	Federal Information Security Management Act.
FPM	Federal Project Manager
FTI	Federal Tax Information
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
HSTS	Not defined in provided RFQ documents. Define at first use per Instructions E.
IaaS	Not defined in provided RFQ documents. Define at first use per Instructions E.
IAL	Identity Assurance Level (IAL). A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

Volume I - Technical Approach

Abbreviation/Acronym	Definition
IAL-1	Identity Assurance Level
IAL2	Identity Assurance Level 2
IAM	Not defined in provided RFQ documents. Define at first use per Instructions E.
IAST	Not defined in provided RFQ documents. Define at first use per Instructions E.
ICT	Information and Communication Technology
IDEA	Not defined in provided RFQ documents. Define at first use per Instructions E.
IFAS	Internet Filing Acceptance Service
IPP	Invoice Processing Platform
IRD	Interface Requirements Document. The governing technical document which describes the requirements applicable to the distribution files pushed to the federal agencies which participate in the EFAST2 program.
IRS	Internal Revenue Service.
ITIC	Industry Technology Industry Council
JSON	Not defined in provided RFQ documents. Define at first use per Instructions E.
LLM	Large Language Model
LOE	Not defined in provided RFQ documents. Define at first use per Instructions E.
MAS	MULTIPLE AWARD SCHEDULE
MBI	Minimum Background Investigation
ML	Machine learning
MPR	Monthly Progress Report
MVP	Minimum Viable Product
NACI	National Agency Check with Inquiries
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NTE	Not to exceed
O&M	Operations and Maintenance
OASAM	Office of the Assistant Secretary for Administration & Management, an agency within DOL which provides the infrastructure and support that enables

Volume I - Technical Approach

Abbreviation/Acronym	Definition
	DOL to perform its mission.
OCI	Organizational Conflict of Interests
OCIO	Office of Chief Information Officer. An office within DOL OASAM dedicated to providing IT solutions and leadership to advance DOL's mission.
OF-306	Not defined in provided RFQ documents. Define at first use per Instructions E.
OIDC	Not defined in provided RFQ documents. Define at first use per Instructions E.
OMB	Office of Management and Budget
PaaS	Not defined in provided RFQ documents. Define at first use per Instructions E.
PATS	Participant Acceptance Testing System. The test environment used to approve and certify third-party transmission and filing software for use with the EFAST2 system.
PBGC	Pension Benefit Guaranty Corporation. PBGC is a federal corporation created by the Employee Retirement Income Security Act of 1974.
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PIC	Not defined in provided RFQ documents. Define at first use per Instructions E.
PII	Personally Identifiable Information. Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in
PIN	Not defined in provided RFQ documents. Define at first use per Instructions E.
PIV	Personal Identity Verification
PMP	Project Management Professional
PN	Plan Number. A unique 3-digit number used to identify the type of plan.
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPM	Not defined in provided RFQ documents. Define at first use per Instructions E.
PROD	Not defined in provided RFQ documents. Define at first use per Instructions E.
PRS	Performance Requirements Summary
PWS	Performance Work Statement. A statement of work for performance-based acquisitions that describes the required results in clear, specific and objective

Volume I - Technical Approach

Abbreviation/Acronym	Definition
	terms with measurable outcomes.
QASP	Quality Assurance Surveillance Plan
RAG	Retrieval Augmented Generation
RFO	Revolutionary FAR Overhaul
RFQ	Request for Quotation
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SaaS	Not defined in provided RFQ documents. Define at first use per Instructions E.
SAM	System for Award Management
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SAST	Not defined in provided RFQ documents. Define at first use per Instructions E.
SAT	Systems Acceptance Test
SCLS	Service Contract Labor Standards
SDLC	Not defined in provided RFQ documents. Define at first use per Instructions E.
SDLCM	Department of Labor's System Development Lifecycle Methodology. The purpose is to ensure automated systems are planned, implemented, modified, and maintained in a manner that meets the program and business needs of the Department with a high degree of reliability, effectiveness, security, and cost efficiency.
SEI	Software Engineering Institute. A federally funded agency with a core purpose of helping others to make measured improvements in their software engineering capabilities.
SEI-CMMI	Software Engineering Institute-Capability Maturity Model Integration. A model for judging the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes.
SIN	Special Item Numbers
SLA	Service Level Agreement
SQL	Not defined in provided RFQ documents. Define at first use per Instructions E.
SSDF	Secure Software Development Framework
SSN	Social Security Number
SSP	System Security Plan

Volume I - Technical Approach

Abbreviation/Acronym	Definition
TAA	Trade Agreements Act
TIFF	Tagged Image File Format
TR	Technical Representative for contract.
U.S.C.	United States Code. A consolidation and codification of all general and permanent laws of the United States.
UAT	User Acceptance Testing
UEI	Not defined in provided RFQ documents. Define at first use per Instructions E.
UI	Not defined in provided RFQ documents. Define at first use per Instructions E.
VPAT	Voluntary Product Assessment Template
WCAG	Not defined in provided RFQ documents. Define at first use per Instructions E.
WPR	Weekly Progress Report
WSDL	Not defined in provided RFQ documents. Define at first use per Instructions E.
XML	Not defined in provided RFQ documents. Define at first use per Instructions E.
XSD	Not defined in provided RFQ documents. Define at first use per Instructions E.

GLOSSARY SOURCE NOTE.

Instructions E: "A glossary of acronyms and terms for each volume must be provided which (including table of contents) will not count against the volume page limit. All acronyms must be defined at first use."

Every acronym above was harvested from the solicitation documents themselves. Definitions marked "Not defined in provided RFQ documents" are acronyms the RFQ uses but never expands; the writer supplies the definition and must still define the acronym at first use in the narrative. Add any acronym your narrative introduces. Delete none that you have used.

Summary Section (Inst. D)

EXCLUDED FROM PAGE LIMIT: the Table of Contents and Summary Section are not included in the page limits, and the Summary Section abstract does not count against the page limits (Instructions D).

INSTRUCTIONS (Instructions to Vendors, D. Content Requirements):

D. Content Requirements All information must be confined to the appropriate volume. The Quoter must confine submissions to essential matters, sufficient to define the quotation details, in a concise manner, to permit a complete and accurate evaluation of each quotation.

Each volume of the quotation must consist of a Table of Contents and Summary Section; these are not included in the page limits. The Narrative discussion, however, does count against the page limits for each volume. The Summary Section must contain a brief abstract of the volume which does not count against the page limits. The quotation volumes must be submitted in Adobe PDF format, with the exception of the price spreadsheet and payment schedule, which must be submitted in Microsoft Excel format. Proprietary information must be clearly marked.

Instructions D, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 154

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

VOLUME I - TECHNICAL APPROACH

FORMAT TRAPS IN THIS SOLICITATION.

1. LINE NUMBERS. Instructions A: "The technical volume must include line numbers on each page." This is Volume I. Turn line numbering on before the PDF is produced. Layout, Line Numbers, Continuous.
2. THE 45-LINE RULE. Instructions C: pages carrying more than forty-five lines of text excluding tables and graphics have the excess lines stripped from back to front and not evaluated. Check line counts on every page, not just the page count.

THE PWS NUMBERING ITSELF CONTAINS THREE DEFECTS THAT AFFECT THIS VOLUME.

1. PWS 5.4.2.3 Transmission Software is printed between 5.4.3.2 and 5.4.3.4 and is plainly intended to be 5.4.3.3. This outline places it in sequence under Third-Party Integration and cites it as the RFQ numbers it, PWS 5.4.2.3.
2. PWS 5.13.7.3 is used twice, for Annual Rollover Updates and for Annual System Maintenance Rollover Changes, with a paragraph duplicated verbatim between them. Both are given headings here and both cite PWS 5.13.7.3.
3. PWS 5.4.5 runs 5.4.5.3 to 5.4.5.5. There is no 5.4.5.4.

1 UNDERSTANDING OF EFAST2 REBUILD/MODERNIZATION REQUIREMENT (INST. VOL I)

PAGE LIMIT: Volume I not to exceed (NTE) 45 pages excluding cover, title page, executive summary, abstract, and table of contents (Instructions C). The limit applies to the whole volume; subheadings below inherit it.

INSTRUCTIONS (Instructions to Vendors, Volume I):

VOLUME I – TECHNICAL CAPABILITY The Vendor must provide a technical narrative in response to Factor I – Technical Capability that *demonstrates its understanding of the EFAST2 Rebuild/Modernization effort and the requirements specified in the Performance Work Statement (PWS) found in Sections 1.3, 1.4, Part 5-Specific Tasks, Technical Exhibit 1- Performance Requirement Summary, and Technical Exhibit 2- Deliverables Schedule*. The narrative must describe the Contractor's proposed methods and approach, including how agile practices will be implemented at DOL to support the agency's mission. The response will be evaluated based on how thoroughly and effectively the Contractor addresses the solicitation requirements and demonstrates the ability to successfully complete the work within the required schedule, without disruption to Government operations or filer services.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 155

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

FACTOR I – TECHNICAL CAPABILITY The Government will evaluate the Vendor’s Technical Capability response to *assess whether the Vendor understands the RFQ, PWS, and associated attachments and can successfully perform the EFAST2 Rebuild/Modernization requirements.*

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 160

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

1.1 Understanding of the Objectives (PWS 1.3)

STATEMENT OF WORK (PWS 1.3):**1.3 Objectives**

DOL is seeking the development and operation of a modernized EFAST application. The Government will utilize the solution approach that best meets the requirement. The solution approach may be either:

- A custom-developed solution deployed in a FedRAMP-authorized cloud environment, such as Amazon Web Services (AWS) or equivalent; or
- A configurable commercial off the shelf (COTS) product (including SaaS, PaaS, or software deployed in the Government’s cloud) that can be tailored via configuration to meet requirements. The application must employ modern technologies and processes to deliver a stable, cost-effective solution within the DOL OCIO environment, designed to support technical and administrative flexibility for future enhancements. The solution must meet requirements for technical performance, security and compliance, usability, interoperability, sustainability, schedule, and risk.

The new EFAST application must meet the following objectives:

1. Enable electronic registration and credentialing for public users to access the filing system, aligned to NIST SP 800-63 digital identity guidelines (e.g., IAL-1, AAL2 for authentication), and integrate with Government-approved identity providers via standards (SAML 2.0 or OIDC/OAuth 2.0).
2. Provide a comprehensive and secure system for filing Form 5500 series and associated forms, including all applicable schedules.
3. Support efficient data collection, processing, and storage for over 1.9 million annual filings for Form 5500 series, Form PR, and Form 5558, with the ability to add additional forms as needed.
4. Pre-populate form information for selected fields based on previous submissions.
5. Create and maintain draft and final versions of annual Government forms, schedules, and instructions based on Government specifications, with versioning and auditability.
6. Provide free web-based software for public filers with the ability to fill out, validate, edit, sign, submit, and amend completed forms. This capability may be provided through configurable COTS/SaaS or custom development.
7. Support bulk filing by the authenticated/authorized third-party software submissions via a Government-approved API. Provide a sandbox, test harness, and certification process. Modernize submissions using a RESTful JSON-based API as the primary intake method, while supporting a phased transition from the

Volume I - Technical Approach

legacy XML system through API versioning, clear data-transformation guidance, and a published deprecation schedule for the legacy.

8. Provide outreach, testing, and support to third-party providers to ensure compatibility and integration.
9. Create and maintain the Data Element Requirements (DER) document and machine-readable artifacts (e.g., JSON/XML schemas), including PDF outputs as required.
10. Control production to ensure all filing submissions successfully complete processing, with automated quality controls, queuing, retries, and exception handling.
11. Provide automated web responses and email acknowledgements to filers following receipt of every filing submission, including status updates and error details where applicable.
12. Process and store data for at least one million filings annually in multiple formats based on different forms and form years; deliver and present filtered data and information to filers, Government agencies, and stakeholders via secure interfaces and APIs.
13. Provide contact center, helpdesk, and tiered support based on Government Furnished Information that explains how to file, troubleshoot common filing errors, answer frequently asked questions, and transfer escalations to Government agencies.
14. Ensure the system is compliant and maintains compliance with the DOL Cybersecurity Policy Portfolio (CPP), NIST SP 800-53 Rev. 5, and applicable OMB policies (e.g., Zero Trust M-22-09; logging M-21-31). For SaaS/PaaS, maintain FedRAMP Authorization at the required impact level; for custom development, support FISMA Authorization to Operate at the required impact level.
15. Implement system improvements based on policy, management, and e-Government directives and initiatives, with a governance process for prioritization and change control.
16. Minimize costs of peak processing times by using auto-scaling in cloud-based technologies and optimizing performance. Work collaboratively with DOL staff and contractors as applicable.
17. Provide the Government with real-time access to monitor operations including quality control, system performance, cost, and contact center data as applicable, with dashboards and APIs.
18. Deliver advanced search and bulk download (APIs & Interface) capability for public and government users and administrative functions for government users; integrate prior filing data to 2009 as requested by the Government.
19. Automatically find and redact PII information in filer attachments before making them available in the Public Search page. Detect PII information in the uploaded files and alert filers to prevent the sensitive data files from being uploaded.
20. Generate comprehensive and automated reports and metrics on EFAST data, Helpdesk calls data and system performance; seek efficiencies to minimize duplicative and manual reporting.
21. Automate acknowledgement of filings, providing filers with electronic status updates for Form 5500/PR/5558 filings.
22. Comply with Section 508 and WCAG 2.1 A and AA accessibility requirements; provide accessibility test results and remediation plans.
23. Ensure data portability and exit planning: enable full export of data, configurations, and audit logs in non-proprietary formats; document processes to transition service without undue burden.

PWS 1.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 12-14

Volume I - Technical Approach

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

1.2 Understanding of the Scope (PWS 1.4)**STATEMENT OF WORK (PWS 1.4):****1.4 Scope**

This outlines the specific areas of work, boundaries, and services covered. The solution must be delivered as a cloud-based service in a Government approved and FedRAMP Authorized (Moderate) environment.

This work involves (1) data collection, processing, and dissemination of Government forms data, (2) support of stakeholders (filers, third-party software, and Government), and (3) management services.

The scope of this work is for the Contractor to deliver the EFAST2 system while meeting the preceding objectives. The scope of the work includes the following:

- Annual Rollover Baseline Changes to operate the system for each processing year and to “rollover” in preparation for succeeding processing year
- Advanced Search & bulk download (API) features on filings
- Contact Center Operations to respond to calls, emails and web inquiries. Includes Chatbot support and user satisfaction analysis (postproduction deployment)
- Program ISO and Support to maintain designated level of system security compliance
- Program Management to maintain a stable management presence for all contractor work activities
- Quality Assurance to establish and maintain a software quality program through all phases of the system development life cycle
- Quality Control to provide an independent quality control unit to measure and report on all performance standards defined in the contract
- Software and License Agreements necessary to support the EFAST2 solution
- Internet Filing Acceptance Service (IFAS) to operate and maintain a high-performance, high-availability, and fully automated service for use by Third Party software
- Performance Monitoring of all system components
- Web Content Management to support a workflow for approved content changes
- Change Management using DevSecOps methodologies
- Third Party Developer Conference to plan and communicate EFAST2 changes (postproduction deployment)
- Non-recurring Rollover Changes to support legislative changes (postproduction deployment) The detailed requirements of developed filing system may be refined adaptively over the course of the effort to continuously meet specified user needs. User needs will be prioritized based on business value and technical dependencies.

PWS 1.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 14-15

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

1.3 Understanding of the Performance Requirements Summary (TE 1)

STATEMENT OF WORK (Technical Exhibit 1):

Technical Exhibit 1 Performance Requirements Summary The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

TE 1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 83-84

Technical Exhibit 1 Group	Standards	Proposed Method of Meeting the Standard
OCIO Performance Requirements	TE1 #1 to TE1 #31	[Insert]
Availability Performance Standards	TE1 #32 to TE1 #36	[Insert]
Accuracy Performance Standards	TE1 #37 to TE1 #41	[Insert]
Timeliness Performance Standards	TE1 #42 to TE1 #63	[Insert]
Quality Performance Standards	TE1 #64 to TE1 #65	[Insert]

Exhibit 1-4. Technical Exhibit 1 Performance Standard Groups (TE 1)

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

1.4 Understanding of the Deliverables Schedule (TE 2)

STATEMENT OF WORK (Technical Exhibit 2):

Technical Exhibit 2 Deliverables Schedule # PWS Section 5 Task Deliverable Due Format Submit To

TE 2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 98

TECHNICAL EXHIBIT 2 NUMBERING SKIPS AND REPEATS.

Technical Exhibit 2 has no TE2#90, and TE2#92 is used twice, once for "Finalized implementation and support documents" and once for "Source code, configurations, etc." Cite deliverables by title as well as by

number so the reference is unambiguous.

Phase (Technical Exhibit 2)	CLIN	Technical Exhibit 2 Deliverables Addressed	Proposed Approach
Phase 1: Transition-In, Discovery & Requirements	0001	[Insert TE2 numbers]	[Insert]
Phase 2: Planning & Architecture	0002	[Insert TE2 numbers]	[Insert]
Phase 3 Sub-Phase 3A: Prototype & Authenticated Applications	0003	[Insert TE2 numbers]	[Insert]
Phase 3 Sub-Phase 3B: Third-Party Support & Public Search	0004	[Insert TE2 numbers]	[Insert]
Phase 4: Integration & Data	1001	[Insert TE2 numbers]	[Insert]
Phase 5: Full System Test, Go-Live & Hypercare	1002	[Insert TE2 numbers]	[Insert]
Phase 6: Post-Modernization O&M (Steady State)	1003, 2001, 3001, 4001	[Insert TE2 numbers]	[Insert]

Exhibit 1-5. Phase and CLIN Alignment (TE 2, SF 18 Schedule)

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

1.5 Understanding of the Deliverable Acceptance Procedures (TE 2)

STATEMENT OF WORK (Technical Exhibit 2, Deliverable Acceptance Procedures):

Deliverable Acceptance Procedures

1. Submission Requirements

The contractor must submit all deliverables in the format, medium, and location specified in the PWS and its technical exhibits. Each deliverable must include version control, document date, and a summary of changes where applicable.

2. Government Review Period

The Government will review each deliverable within the timeframe defined in the PWS or associated technical exhibits. Unless otherwise stated, the standard review period is ten (10) business days from receipt.

3. Acceptance Criteria

Deliverables will be assessed against the performance standards, quality requirements, and measurable outcomes defined in the PWS, Performance Requirements Summary (PRS), and Quality Assurance

Volume I - Technical Approach

Surveillance Plan (QASP). These criteria include completeness, accuracy, compliance with applicable security and accessibility requirements, and alignment with system, functional, or operational needs.

4. Deficiency Notification

If a deliverable is found inadequate or non-compliant, the Government will issue written notice identifying the deficiencies. The contractor must correct the deficiencies and resubmit the deliverable within the period specified by the Government.

5. Resubmission and Final Acceptance

Upon resubmission, the Government will re-evaluate the deliverable for compliance with all acceptance criteria. Final acceptance will be issued in writing once the deliverable meets all requirements.

6. Failure to Meet Requirements

If the contractor fails to provide an acceptable deliverable after resubmission, the Government may take action consistent with the contract, including withholding payment associated with the deliverable, documenting performance concerns, or applying other remedies outlined in the QASP.

7. Government Rights in Deliverables

All deliverables must be provided with Government-reserved rights consistent with FAR data-rights clauses applicable to the contract. Source code, configuration artifacts, documentation, and other data required to support continuity, transition, or future maintenance must be provided as described in the PWS and transition requirements.

TE 2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 105-107

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2 TECHNICAL APPROACH, METHODS, DEVELOPMENT PRACTICES, AND TOOLS (INST. VOL I)

INSTRUCTIONS (Instructions to Vendors, Volume I):

The Vendor must submit a quotation that demonstrates a clear understanding of the RFQ, PWS, and the EFAST2 Rebuild/Modernization objectives, scope, and key requirements. ***The response must describe the Vendor's technical approach, methods, development practices, and tools for performing the work across the multi-platform enterprise environment, including design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration.*** The Vendor must address functional, security, and compliance requirements; identify key risks and credible mitigation strategies; and demonstrate relevant experience of similar nature, scope, complexity, and risk. The response must also describe the Vendor's familiarity with large-scale federal IT modernization efforts and its approach to assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition. General or vague statements without supporting rationale or examples will not be sufficient.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 155-156

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The evaluation will consider the clarity, completeness, feasibility, and credibility of the proposed technical approach, including the Vendor's understanding of the scope of work, required technologies, methodologies, standards, and ability to manage performance risk. The Government will assess how the proposed solution addresses functional, security, and compliance requirements, including FedRAMP, FISMA, NIST SP 800-53 Rev. 5, IRS Publication 1075, identity management and authentication, and Section 508 and WCAG 2.1 A/AA accessibility. The evaluation will also consider the Vendor's use of AI, automation, DevSecOps, agile practices, and innovative solutions to support development, modernization, operations, and enhancement activities; reduce delivery time; maintain secure and current software; minimize vulnerabilities; and ensure continued compliance with Federal requirements.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 160

HOW THIS SECTION IS ORDERED, AND HOW THE THIRTEEN NAMED TOPICS ARE COVERED.

The subheadings below follow the Performance Work Statement's own sequence, PWS 5.1 through 5.14, with every parent paragraph keeping its own subparagraphs. Nothing in the RFQ mandates a response order; Instructions A requires only that the submission be "clearly indexed and logically assembled," and mirroring the Government's own document is the most defensible reading of that.

The Instructions paragraph quoted above names thirteen topics: design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration. Every one is covered below. They are a coverage checklist, not an outline: the RFQ presents them in a prose sentence and never asks for them in that order.

Where each is answered: design PWS 5.3 and 5.5; development PWS 5.4; architecture PWS 5.13.8; DevSecOps PWS 5.11; AI and innovative solutions PWS 5.4.5 and 5.8.2; security and compliance PWS 5.13.3 and Section 3 of this volume; operations and maintenance PWS 5.13; contact center support PWS 5.8; filing acceptance services PWS 5.4.2; third-party integration PWS 5.4.3; annual rollover PWS 5.13.7; data dissemination PWS 5.6; data migration PWS 5.9. Record each mapping in the cross-reference matrix that Instructions E requires.

DEPTH VERSUS THE PAGE LIMIT. This section carries one heading for every numbered PWS Part 5 paragraph. The volume is capped at 45 pages. Writers may consolidate adjacent headings where one narrative answers several paragraphs, but every PWS paragraph listed here must remain covered somewhere in the volume and traceable in the cross-reference matrix. **Do not drop coverage to save pages.**

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.1 Transition-In and Assumption of Full Contractual Responsibility Within Thirty Days of Award (PWS 5.1, Inst. Vol I)

STATEMENT OF WORK (PWS 5.1):

5.1 Transition-In

The Transition-In is to allow the incoming contractor to staff up to the appropriate support levels, participate in knowledge sharing with EBSA and OCIO stakeholders, and to be able to fully support the contract requirements within 30 days. During this time, the Contractor must go through an onboarding process which includes background investigations to obtain DOL badges, DOL laptops, access to DOL's systems and network, and applicable government furnished information (GFI). DOL expects the contractor to mobilize all staff and other resources, so the workforce is functional and operational within 30 calendar days of contract award.

The Contractor must perform the following Transition-In tasks:

- Onboard contractor employees, i.e., complete background screening, obtain DOL PIV badges, complete applicable security training, obtain laptops, obtain network and systems access, sign confidentiality agreements if applicable.
- Ensure contractor employees understand their roles and responsibilities along with the requirements of this effort, i.e., deliverables/timelines, Agile framework, deployment environment and required templates, DOL OCIO processes, etc.
- Interview the COR, PM, and/or business stakeholders to fully understand and assess the EFAST 2 Application being developed, as well as applicable documentation.
- On request from CO/FPM, attend Technical Exchange Meetings (TEMs) with the O&M contractor to gain knowledge of the systems and activities, including sustainment.
- Ensure an understanding of the existing systems documentation, backlog, requirements, source code,

Volume I - Technical Approach

systems architectures, and planned releases.

- Provide a list of anticipated software necessary to support this task order to the COR/PM.
- Report Transition-In activities, risks, and issues during regular status meetings.

PWS 5.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 40-41

INSTRUCTIONS (Instructions to Vendors, Volume I):

The Vendor must submit a quotation that demonstrates a clear understanding of the RFQ, PWS, and the EFAST2 Rebuild/Modernization objectives, scope, and key requirements. The response must describe the Vendor's technical approach, methods, development practices, and tools for performing the work across the multi-platform enterprise environment, including design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration. The Vendor must address functional, security, and compliance requirements; identify key risks and credible mitigation strategies; and demonstrate relevant experience of similar nature, scope, complexity, and risk. The response must also describe the Vendor's familiarity with large-scale federal IT modernization efforts and ***its approach to assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition.*** General or vague statements without supporting rationale or examples will not be sufficient.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 155-156

TRANSITION-IN IS SHARED WITH VOLUME II - WRITE A SHORT CONFIRMATION HERE, NOT THE FULL APPROACH.

Instructions, Volume II names this paragraph directly: the management response must "describe its approach to assuming full contractual responsibility within thirty (30) days of award, including Transition-In, continuity of operations, and post-modernization support with no disruption or degradation of service." Evaluation Factor II grades "Start-Up, Transition-In, and Transition-Out approaches."

Volume I's own ask is narrower. Instructions, Volume I requires the approach to "assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition," and Evaluation Factor I grades it "with minimal Government involvement in knowledge transition."

WRITE HERE: a short passage that (1) demonstrates understanding of the PWS 5.1 Transition-In requirements quoted above, (2) answers Volume I's narrow angle - how knowledge transition is achieved with minimal Government involvement inside thirty days - and (3) states plainly that the full Transition-In management, staffing and continuity approach is provided in Volume II - Management Approach.

DO NOT put the staffing plan, hiring approach or management structure here. Instructions F: information required for evaluation that is not found in its designated volume "will be assumed to have been omitted from the quotation."

THE THIRTY-DAY CLOCK IS TIGHT. Quotes are due 14 September 2026 and the base period begins 25 September 2026. PWS 5.1 requires the workforce "functional and operational within 30 calendar days of contract award." Background investigations, PIV badging and DOL network access all sit inside that window. Show the sequencing.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.2 Project Management Services and Implementation of Agile Practices at DOL (PWS 5.2, Inst. Vol I)

STATEMENT OF WORK (PWS 5.2):

5.2 Project Management Services

The contractor must provide agile project management services for application design, development, deployment and testing as directed and managed by the DOL Federal Project Manager (FPM). The Contractor is supporting the Government and managing the tasks to which they have been assigned. The Contractor's Project Manager (PM) ensures support to accomplish their tasks. The Contractor's project management will ensure that tasks and activities are coordinated and successfully executed.

This includes, but is not limited to:

- Support, monitor, and manage activities of the project through its lifecycle.
- Coordinate with the government to refine and anticipate needs to ensure appropriate team size and composition.
- Resource the project with qualified individuals, services, and materials.
- Consistently provide high quality, timely, and professional deliverables.
- Accomplish contract activities within budget.
- Leverage contractor resources for thought-leadership, research, and suggesting best practices.
- Assess requirements and provision resources to meet those needs.
- Manage relationships among its team members.
- Maintain an integrated project schedule.
- Provide financial and project activity analysis leveraging a variety of tools, information systems, and reporting formats.
- Manage delivery of all deliverables and reporting requirements.
- Maintain quality control throughout the duration of the contract through repeatable, managed processes.
- Work collaboratively with DOL stakeholders and OCIO SORT team to maintain a target architecture.

The Contractor must coordinate actively and responsively with the Government and other Government-designated vendors participating in the design, development, test, implementation & deployment of the EFAST 2 application. Failure or refusal to coordinate and cooperate with other DOL Contractors precludes

Volume I - Technical Approach

effective performance of this task.

As requested by DOL, the contractor must:

- Provide input and assistance to the FPM to help evaluate potential changes to the system (e.g., providing options, recommendations, level of effort (i.e., cost), and schedule estimates.
- Post at a DOL Teams Site, DOL SharePoint Site, and/or Confluence location all system documentation.
- Provide updates for all project artifacts required by the Government and be responsible for moving the project through the stage gates by completing all requirements identified in each stage's checklist.
- Maintain a risk register which identifies risks and mitigation plans, and provides for special emphasis on cost controls, time management, continuous improvement, and ongoing contract monitoring.
- Maintain a project review process where, on a scheduled basis, the project manager provides status reports demonstrating cost performance, schedule performance, resource management, achievements, and projections.
- In conjunction with the FPM, maintain a PM workbook containing burn up charts, cost variance worksheets, hour projection worksheets, personnel reports, off duty escalation contact information, GFE equipment inventory, logical access lists, etc.
- Provide invoice detail reports including monthly burn-rate projections which form the basis for actual costs reported and tracked in the integrated baseline plan and for earned value management performance monitoring.
- Provide hour usage breakdown by individual name to include hours worked and Labor Category of each employee.
- Provide a contract personnel report which includes all personnel working on the contract and those who have departed the contract. Information must include at a minimum, name, work telephone number, work email address, home contact info, GFE make/model/serial number, virtual telephone number, duty description, certifications/qualifications as required by role, work schedule, extended time off.
- Provide an escalation list of contract team off duty contact info, mobile phone, and email, to be used in case of unexpected issue or urgent communication. The escalation list must contain at least one corporate Point of Contact (POC).
- Track the allocation and consumption of funds on the contract and provide advanced warning of funding shortfalls using financial burn rate charts.
- Identify and communicate to the Government all necessary software, hardware, licenses, or equipment required in support of the performance of this contract.
- Work collaboratively with DOL stakeholders to create and maintain documentation in support of Enterprise Architecture and Capital Planning & Investment Control.
- Provide DOL stakeholders with formal briefings as requested.
- Provide regular status briefings for the FPM.
- Include PM on all communications with Government or industry stakeholders.
- Provide bi-weekly sprint planning, backlog grooming/refinement, daily SCRUM, sprint retrospective, and other meetings as directed and approved by the FPM.
- Include PM on all communications with Government or industry stakeholders.
- Provide bi-weekly sprint planning, backlog grooming/refinement, daily SCRUM, sprint retrospective, and other meetings as directed and approved by the FPM.

Volume I - Technical Approach

PWS 5.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 41-43

INSTRUCTIONS (Instructions to Vendors, Volume I):

VOLUME I – TECHNICAL CAPABILITY The Vendor must provide a technical narrative in response to Factor I – Technical Capability that demonstrates its understanding of the EFAST2 Rebuild/Modernization effort and the requirements specified in the Performance Work Statement (PWS) found in Sections 1.3, 1.4, Part 5-Specific Tasks, Technical Exhibit 1- Performance Requirement Summary, and Technical Exhibit 2-Deliverables Schedule. The narrative must describe the Contractor's proposed methods and approach, **including how agile practices will be implemented at DOL to support the agency's mission.** The response will be evaluated based on how thoroughly and effectively the Contractor addresses the solicitation requirements and demonstrates the ability to successfully complete the work within the required schedule, without disruption to Government operations or filer services.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 155

PROJECT MANAGEMENT IS SHARED WITH VOLUME II - WRITE A SHORT CONFIRMATION HERE, NOT THE FULL APPROACH.

Instructions, Volume II names this work directly: "Management Approach: Describe the management structure, tools, processes, risk management approach, communication methods, and coordination with Government stakeholders." Evaluation Factor II grades the "organizational structure, management techniques, tools, and processes for organizing the work, overseeing task orders, managing schedule and budget performance."

Volume I's own ask is narrower. Instructions, Volume I requires the narrative to describe the proposed methods and approach "including how agile practices will be implemented at DOL to support the agency's mission." Evaluation Factor I grades the Vendor's use of "AI, automation, DevSecOps, agile practices, and innovative solutions."

WRITE HERE: a short passage that (1) demonstrates understanding of the PWS 5.2 requirements quoted above, (2) answers Volume I's narrow angle - how agile practices, two-week sprints, ceremonies and the Jira toolchain are implemented at DOL - and (3) states plainly that the management structure, risk management and stakeholder coordination approach is provided in Volume II - Management Approach.

DO NOT put the organisational chart, management structure or the Quality Control Plan here. Instructions F applies.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.2.1 Monthly Progress Report (MPR) (PWS 5.2.1)

STATEMENT OF WORK (PWS 5.2.1):

5.2.1 Monthly Progress Report (MPR) The Contractor must prepare and deliver a Monthly Progress Report to the COR and FPM. The MPR must outline deliverables submitted, problems encountered, and schedule deviations.

PWS 5.2.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 43

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.2.2 Weekly Progress Report (WPR) (PWS 5.2.2)

STATEMENT OF WORK (PWS 5.2.2):

5.2.2 Weekly Progress Report (WPR) The Contractor must prepare and deliver a Weekly Progress Report (WPR) to the FPM. The WPR must summarize the tasks and activities being worked on and their status of completion; this report must cover each Monday through Friday period and is due by the close of business on the first business day of the next period.

PWS 5.2.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 43

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.3 Design & Prototype Development (PWS 5.3)

STATEMENT OF WORK (PWS 5.3):

5.3 Design & Prototype Development

The contractor must provide iterative design and development services with a focus on data repository design, UX design, EFAST data collection, filing processing, validating and PII/FTI data security, and prototype development.

Key goals:

- Initial architecture technical and data design.
- Set up the development and test environments for prototyping.
- Initial wireframe for at least one form (Form 5500 with one schedule at least) completed and approved by government.
- Data collection, storing, validating, processing and data distribution for at least one form (Form 5500 with

one schedule at least).

- A database design for EFAST data and secured design for PII/FTI data storage for Form 5558.
- Integrating with login.gov supporting IAL-1.

Deliverables:

- Approved initial wireframe concept design.
- Development and Test environments operational.
- Architecture design of application and support for PII/FTI data and documents.
- Approved landing page with login.gov integration.
- One of 5500 series form is submitted through web interface and API and validated with current data structures supported by 3rd Party vendor.

Performance Metrics:

- Wireframe for all user interfaces approved by stakeholders.
- 100% operational development and test environment
- Completed architecture diagrams for the application and data
- A working landing page and integration with login.gov supporting IAL-1.
- Working functionality for one of the 5500 forms to collect data, validate supporting existing data structures and store the data.

PWS 5.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 43-44

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4 Design & Development (PWS 5.4)

STATEMENT OF WORK (PWS 5.4):

5.4 Design & Development

The Contractor must design, develop, and implement a complete system for electronic filing of Form 5500 series (Form 5500, 5500 SF, 5500-EZ) returns, Form PR and 5558 form. The electronic filing requirements are structured as outlined in following sections:

PWS 5.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 44

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.1 Registration Portal (PWS 5.4.1)**STATEMENT OF WORK (PWS 5.4.1):**

5.4.1 Registration Portal The contractor must design and develop a registration portal that integrates with Login.gov with IAL-1 for the filer to securely login and access to perform filing related activities such as filing, signing, amending previous filings, search and other functionalities determined from the technical exchanges, requirement discussions and existing documentation.

There are three types of applicants: filing transmitters, signers, and web portal users. A transmitter is an authorized individual or organization that submits electronic returns for a plan, requiring them to obtain an ID and PIN through the Registration Process to submit filings. The transmitter does not have to be the same as the plan administrator or employer.

The signers include three groups:

- Plan Administrators must obtain an ID and PIN to electronically sign Form 5500.
- Employers/Plan Sponsors similarly need ID and PIN credentials for signing Form 5500.
- DFEs must also apply for ID and PIN to sign Form 5500 on behalf of the DFE.

The same ID and PIN can be used for signing and transmitting filings, but batch transmitters (organizations submitting multiple filings) need different credentials not used for signing. Individuals accessing authenticated services via the web portal should apply for an ID and PIN through “web-based filing application.” Third-party attestors like actuaries and accountants can apply for credentials to authorize certain filing portions but are not required to do so. There can be one to three signatures on a filing (plan administrator, employer/plan sponsor, and/or DFE). When filing, the preparation software will apply the signer’s credentials, including their ID, PIN, name, and date. These credentials will be authenticated against

the database upon submission. The filing software must ensure that each signatory's PIN remains confidential and only accessible to them, a requirement verified through the Contractor's certification program.

The Contractor will create a web-based application for registration in electronic filing, requiring participants to apply for Plan Year 2009 and later. The registration will verify the identity of the applicant, who must provide certain contact information, including their full name, mailing address, daytime phone, optional fax, and email. Applications must be completed in one session, as incomplete applications will not be saved. The Contractor will implement measures to protect against automated registration attempts that could disrupt the service.

PWS 5.4.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 44-45

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.2 Filing Acceptance Service (PWS 5.4.2)

STATEMENT OF WORK (PWS 5.4.2):

5.4.2 Filing Acceptance Service

The Contractor must develop an auto-scalable, high-performance, high-availability, and fully automated “Filing Acceptance Service” for accepting and processing electronic filing submissions including forms, schedules, and attachments, in electronic form based on XML standards or Government approved standards to support the processing of Form 5500 series filings and 5558 Form. It is not applicable for Form PR.

The service must receive electronic filing submissions from EFAST2-approved third-party software or its free, direct filing web interface Filing web-based application. Approximately one (1.1) million filings are typically submitted annually. Between 10%-20% of filings are typically submitted through “web-based filing application” while the vast majority of filings are submitted through third-party software.

Submissions from third-party software may include multiple filings in a single batch transmission.

The “Filing Acceptance Service” must first determine if a submission is processable. Then “Filing Acceptance Service” must determine the filing status of each filing in a processable submission.

All submissions must be completed and resolve to a final status.

PWS 5.4.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 45

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.2.1 Filing Submission Flow (PWS 5.4.2.1)

STATEMENT OF WORK (PWS 5.4.2.1):

5.4.2.1 Filing Submission Flow

The Filing Acceptance Service must be designed to manage the electronic submission process efficiently. Initially, the service will archive the original requests as "Processing," parse them into individual filings, and create corresponding records in a Tracking Database for each filing. It will validate the Form Year and Filing elements against established business rules (Refer schemas as specified in the Government-approved Data Element Requirements (DER)), ensuring that all binary attachments are valid PDFs. Any failures in validation will necessitate termination of processing with an appropriate unprocessable status.

Furthermore, the service will run validation rules to categorize errors based on severity, resulting in appropriate filing status records, such as Processing Stopped, Error, or Filing Received. It will determine the filing type, authenticate signatures in the Filing Header, and track the results accordingly. Submissions will only be accepted through valid web service requests that comply with government approved data standards while supporting XML standards currently accepted by the EFAST system. All requests must originate from EFAST2-approved third-party products equipped with valid vendor credentials and must also be virus-free to avoid processing termination.

To maintain compliance, the web service must support all form years and versions related to the Form 5500 series and Form 5558, alongside their respective schedules and attachments. Additionally, the contractor is tasked with developing validation rules/edit tests outlined in the DER, including checks for masked edits and incorrect filings. Specific web service protocols must be established for tracking amended filings by

Volume I - Technical Approach

requiring the original filing's Acknowledgement Id, thereby enabling accurate linking and timestamping of amendments.

The service will implement a Cross-Year Entity Validation Model to ensure consistency across filing years, thereby matching key entity fields against previous submissions. Detailed filing status records will be maintained in a secure database, tracking any failed edit or schema tests. Lastly, automated notifications will be sent to filing signers, authors, and transmitters of submissions, providing key filing data with an option for recipients to opt out of email communications.

PWS 5.4.2.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 45-46

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.2.2 Filer Authentication (PWS 5.4.2.2)

STATEMENT OF WORK (PWS 5.4.2.2):

5.4.2.2 Filer Authentication

The Contractor must implement a routine for filers to authenticate to electronically sign filings and authenticate to the EFAST2 website. Note that there can be one or more signatures provided on a single filing.

Identity Assurance Level (IAL-1) must be used for enrollment and identity proofing of the web portal authentication and electronic signatures. Authentication Assurance Level (AAL) 2 must be used for filer authentication of the web portal authentication. Identity Assurance Levels are defined by NIST SP 800-63 series.

To achieve AAL2, NIST SP 800-63 requires the enforcement of Multi-factor Authentication (MFA). The Contractor must integrate Login.gov as a secure sign-in service, at IAL-1 with multi-factor authentication into the EFAST2 web portal. All web portal users must be required to use Login.gov integrated authentication to access the EFAST2 web portal in a phased approach subject to Government approval. Filer authentication should include an attribute indicating if the authorized individual is a current Government employee (EBSA, IRS, OCA, PBGC, COR or COR representative).

EFAST2 must obtain and authenticate filer identity to the extent feasible and practical using Government-approved methods. The contractor must maintain user stories or use cases or similar documentation illustrating the filer authentication routine, including filer identity information collected/stored/passed. Any filer authentication credentials issued/stored by the contractor must be encrypted while in transit and at rest.

A filing credential may be deemed compromised if an unauthorized individual has obtained it. If this is reported, the contractor must revoke the credential. No filing will be accepted using a revoked credential. In the event of revoked credentials, the Contractor must offer to transfer previous filings to a new account should the user need to retain access to their previous filing information in accordance with Government-approved procedures.

Filer accounts may only be locked/revoked by the Contractor based on valid user requests.

PWS 5.4.2.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 46-47

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3 Third-Party Software Support (PWS 5.4.3)

STATEMENT OF WORK (PWS 5.4.3):

5.4.3 Third-Party Software Support

The Contractor must implement a support program for third-party software developers and providers, and test and approve third-party software on behalf of the Government. It is vital that third-party software used to create and transmit filings to EFAST2 does so in strict accordance with Government-published schemas and communications protocols.

Also, to reduce the incidence of unprocessable submissions, the Government encourages third-party software to pre-validate filings prior to submission. The Contractor reviews and responds to questions and feedback about the system and /or Specifications. These questions are reviewed and shared with the Government. In addition, the Government needs to ensure that third-party software protects the integrity and privacy of electronic signatures. The Contractor's testing and certification procedures must be the Government's primary means of ensuring these capabilities of approved third-party software.

The Contractor must ensure that the most current version of Government-approved third-party software support material are available on the EFAST2 website. This includes test filing data, the Guide for Filers and Service Providers, the Software Developer's Specification and additional specifications in support of software developers, including, but not limited to, the Data Element Requirement (DER) and the business rules (edit test) mask lists for all previous form years.

The Contractor must provide technical support necessary to aid applicants in the successful completion of certification procedures, working with them until their product is approved. The Contractor may conduct multiple rounds of certification testing with a software developer.

In some cases, individual forms and schedules may be created using other non-certified software prior to assembly into a complete, signed filing. However, the software used to apply the electronic signatures to the assembled filing must be approved and certified, as authenticated by the valid vendor's credential.

The Contractor must ensure third-party software support and specifications are developed to induce the widest range of participation by software providers. If the Contractor provides a third-party software product in addition to the free "web-based filing application" service, the Contractor must ensure that the Contractor's software provider group has no advantage over other third-party software developers (e.g., early software development or certification, shared code, information testing, etc.).

PWS 5.4.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 47

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.1 Third-Party Software Certification Criteria (PWS 5.4.3.1)**STATEMENT OF WORK (PWS 5.4.3.1):*****5.4.3.1 Third-Party Software Certification Criteria***

The Contractor must establish processes and procedures for third-party software testing, assist in the certification process, and award certification credentials as specified in this work statement, all subject to Government review and approval. To facilitate compliance, the Contractor must also implement a self-certification mechanism for the involved third-party vendors, enabling them to confirm their adherence to the certification requirements. Additionally, alternative validation methods, such as signed affidavits or direct inspections, must be developed for cases where software capabilities cannot be verified through test filings. Any affidavits should clearly state that the respondents have the authority to represent the software provider in their declarations.

To ensure a reliable certification process, the Contractor must maintain documented agreements with software providers that define the type and duration of the certification. This documentation should be retained until the software is no longer certified, and agreements must ensure that authorized signatories comply with EFAST2 certification requirements annually. Furthermore, the Contractor is responsible for alerting the Contracting Officer's Representative (COR) to any noncompliance issues and will take necessary actions to disallow non-compliant software from participating as certified providers, following COR's approval.

PWS 5.4.3.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 47-48

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.2 Filing Preparation Software Test Scenarios (PWS 5.4.3.2)**STATEMENT OF WORK (PWS 5.4.3.2):*****5.4.3.2 Filing Preparation Software Test Scenarios***

The Contractor is required to develop up to 10 comprehensive test scenarios for filing preparation software, covering a range from simple EZ filings to complex DFE filings with multiple schedules and attachments. Each scenario must list the relevant forms, schedules, and attachments in a straightforward Excel or PDF format. Key scenario requirements include incorporating all EFAST2 schedules and including scenarios for multiple Schedule A's and Schedule DCG's, a large defined benefit plan, a welfare plan, a DFE filing, a terminated plan, an amended filing, an extension, an Accountant's Opinion, a text attachment, and a user-defined "Other Attachment" type.

Using the test scenarios, software providers will create, sign, and submit filings to the test environment via approved transmission software. The test environment facility will validate submissions using the same processes as the production EFAST2 system, ensuring the software produces schema-valid data and attachments handled correctly. The Contractor must implement a mechanism for providers to electronically access their filing status.

To obtain certification, providers must achieve correct status for all scenarios and submit one complete error-free batch after certification. Additionally, the software must provide access to official Government

filer instructions and ensure schema validation and virus checks on attachments. The software must also maintain secure electronic signatures, preventing edits after signing and ensuring authorized access to filing header information while masking personal identification numbers (PINs) for confidentiality.

PWS 5.4.3.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 48

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.3 Transmission Software (PWS 5.4.2.3)

STATEMENT OF WORK (PWS 5.4.2.3):

5.4.2.3 Transmission Software

The Contractor must test third-party software for transmitting filings and filing status requests to EFAST2, certifying compliance with Government requirements and compatibility with “Filing Acceptance Service”, with certification indicated by valid vendor credentials. This certification does not include testing for filing acceptance and remains valid unless significant changes are made to the transmission protocol; the Government may require recertification if issues arise. The Participant Acceptance Test System (PATs) Package will provide software providers with government approved data format files while supporting the XML format files, representing valid filings and necessary data elements for testing, including at least one filing with PDF attachments. Functionality testing will ensure the software can successfully transmit service requests and handle operational responses, including creating and assembling the request message correctly. The Contractor must verify the software’s capabilities, such as schema validation before transmission, virus checks on attachments and generating printable receipts and error reports. Additionally, documentation of the host environment must be provided to ensure all prerequisites are met for software installation.

PWS 5.4.2.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 48-49

THIS PARAGRAPH IS MIS-NUMBERED IN THE SOLICITATION.

PWS 5.4.2.3 Transmission Software is printed between 5.4.3.2 and 5.4.3.4 and is plainly intended to be 5.4.3.3. It is placed here in its correct sequence under Third-Party Software Support and cited as the RFQ numbers it.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.4 Third-Party Software Authorization (PWS 5.4.3.4)**STATEMENT OF WORK (PWS 5.4.3.4):****5.4.3.4 Third-Party Software Authorization**

The Contractor must establish and maintain an authorization routine for third-party software vendors, enabling them to electronically authenticate to the EFAST2 Participant Acceptance Test System (PATs) and production environments while agreeing to software rules through an affidavit. Multiple representatives from a single company may be attributed to a specific software product using Vendor credentials, and identity proofing will utilize Identity Assurance Level (IAL-1) and Authenticator Assurance Level (AAL) 2 as defined by NIST SP 800-63. All authentication credentials issued by the Contractor must be encrypted both in transit and at rest, with documentation maintained to illustrate the authentication routine and the identity information collected.

PWS 5.4.3.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 49

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.5 Third-Party Software Developer Conference (PWS 5.4.3.5)**STATEMENT OF WORK (PWS 5.4.3.5):****5.4.3.5 Third-Party Software Developer Conference**

The Contractor must organize an annual software developer conference to discuss changes to forms, business rules (referred as edit tests), and communications protocols, while also soliciting feedback on XML Schema and/or government approved data format and transmission specifications. The conference will focus on electronic filing specifications and certification procedures, with topics of interest to the developer community submitted for Government approval. Additionally, special topics may include the analysis of edit tests, unprocessable error failures, and common inquiries from the contact center.

PWS 5.4.3.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 49

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.6 Guide for Filers and Service Providers (PWS 5.4.3.6)**STATEMENT OF WORK (PWS 5.4.3.6):****5.4.3.6 Guide for Filers and Service Providers**

The Contractor must create, modify and deliver the EFAST2 Guide for Filers and Service Providers. The Guide for Filers and Service Providers must provide helpful information regarding EFAST2 filing

processes and procedures. The audience for this guide is filers, preparers, and other service providers.

PWS 5.4.3.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 49

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.7 Software Developer's Specification (PWS 5.4.3.7)

STATEMENT OF WORK (PWS 5.4.3.7):

5.4.3.7 Software Developer's Specification

The Contractor must maintain and update the "EFAST2 Specification for Software Developers" to reflect any necessary technical changes impacting software development. This specification will include essential details for developing software that authors and transmits electronic filings, covering areas such as XML schema and/or government approved data format, data elements, user interface requirements, and communications protocols. Revised versions will clearly highlight changes in a change table, ensuring third-party developers have the necessary descriptions of file specifications and validation criteria for certified software.

PWS 5.4.3.7, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 49

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.8 Participant Acceptance Testing System (PATs) Test/Certification Program (PWS 5.4.3.8)

STATEMENT OF WORK (PWS 5.4.3.8):

5.4.3.8 Participant Acceptance Testing System (PATs) Test/Certification Program

The Contractor must establish a program to test third-party EFAST2 software packages, certifying that they can create valid filing data and effectively communicate with EFAST2. This testing program will enable software developers to self-test their applications and automatically obtain detailed filing status information.

To maintain consistency, the message validation criteria and error reporting will mirror those used in the production system as closely as possible. The certification process will cover several critical aspects, including the creation of message headers for web services, successful communication with the "Filing Acceptance Service", and the generation of valid XML and/or government approved data format filing data. It will also assess the protection of filing header information, the transmission of test filings, the handling of attachments, and the receipt of response and fault messages. Upon successful completion of

Volume I - Technical Approach

PATS testing, the Contractor will award each software package Vendor credentials as a certification credential, maintaining a database of valid IDs for each Form Year. Notably, the Vendor credentials is specific to a software product and must be renewed annually or when substantial changes to the software affecting data structures occur; the Contractor will also allow vendors to submit a list of exceptions for limited certification of specific forms or schedules.

PWS 5.4.3.8, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 49-50

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.9 PATS Test Filings (PWS 5.4.3.9)**STATEMENT OF WORK (PWS 5.4.3.9):****5.4.3.9 PATS Test Filings**

The Contractor must implement and deliver PATS test filings and make those available to third-party software developers. PATS test filings must be patterned after prevailing comparable electronic filing PATS test filings under the EFAST2 program. At a minimum, the PATS test filings must provide software developers with a set of real-world test filings that exercise the full range of Form 5500 series forms, schedules, attachments and filer entries expected during live processing. Each year, the test filings should be updated to include new and/ or modified data fields that will be implemented during the coming rollover.

PWS 5.4.3.9, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 50

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.10 Third-Party Software Test Plan and Certification Procedures (PWS 5.4.3.10)**STATEMENT OF WORK (PWS 5.4.3.10):****5.4.3.10 Third-Party Software Test Plan and Certification Procedures**

The Contractor must implement, modify and deliver procedures for third-party software providers to apply for certification, conduct testing, and receive their applicable credentials. These procedures must address such items as how to complete a certification package, how to submit a certification package, how to create and transmit valid test submissions, and how to obtain and apply the certification credentials.

PWS 5.4.3.10, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 50

Volume I - Technical Approach

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.11 Annual Updates and Certifications (PWS 5.4.3.11)**STATEMENT OF WORK (PWS 5.4.3.11):*****5.4.3.11 Annual Updates and Certifications***

The Contractor must create and update software developer support materials at least annually in response to annual forms and other system changes. This update must allow software developers and service providers sufficient time to make changes prior to the date of annual rollover. The Contractor must require certification of filing software for each form year.

PWS 5.4.3.11, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 50

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.3.12 Software Developer Monitoring (PWS 5.4.3.12)**STATEMENT OF WORK (PWS 5.4.3.12):*****5.4.3.12 Software Developer Monitoring***

The Contractor must implement mechanism to actively monitor filing submissions to the EFAST2 production system to ensure third-party compliance with all stated certification and affidavit requirements. This includes, but is not limited to, schema and edit test error rates by developer. In instances where the Contractor identifies anomalies in third-party software developer submissions, the Contractor must work directly with the third-party software developer to resolve these issues. The Contractor must notify the Government of any and all anomalies and provide documentation and analysis with respect to the observed anomaly, root cause, resolution and suggested steps for future mitigation of the problem.

PWS 5.4.3.12, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 50-51

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4 Filing Guidelines (PWS 5.4.4)**STATEMENT OF WORK (PWS 5.4.4):*****5.4.4 Filing Guidelines***

PII Redaction Process The Contractor must propose and implement after government approval a fully automated PII detection and redaction solution that scans all filing attachments prior to public release, automatically redacts detected sensitive PII including but not limited to SSNs, bank account numbers, PINs, and legacy security challenge responses and routes flagged attachments to a human-in-the-loop PII Review Process queue. Flagged attachments must be automatically withheld from public search until the review is complete. Upon detection, the system must immediately notify the filer via automated alert, enabling corrective action prior to public disclosure. The redaction engine must operate exclusively on attachment content, ensuring no structured form or schedule data is altered. The authenticated filer portal must provide role-based access enabling filers to view both the original and redacted versions of their publicly disclosed submissions at any time.

PWS 5.4.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 51

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.1 Unauthenticated User Applications (PWS 5.4.4.1)

STATEMENT OF WORK (PWS 5.4.4.1):

5.4.4.1 Unauthenticated User Applications

The Contractor must propose and develop an advanced search application for unauthenticated public users to find, view, download through API, download from the search page and print publicly disclosable Form 5500 and 5500-SF filing records using search and filter criteria based on form and schedule fields, with Government-approved instructions, help text, and aids maintained throughout. Only the most recent amendment must be disclosed when multiple amendments exist; original filings must not be disclosed upon amendment submission.

PWS 5.4.4.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 51

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.2 PII Review of Flagged Attachments (PWS 5.4.4.2)

STATEMENT OF WORK (PWS 5.4.4.2):

5.4.4.2 PII Review of Flagged Attachments

The contractor must propose and implement a solution that publicly discloses the structured data (Form 5500/5500-SF, schedules, and Form 5500-EZ) with “Attachment(s) Under Review” while the flagged attachments are being reviewed in the PII Review Process. The contractor must ensure that no attachment must be publicly accessible while it is under review. Unstructured attachments deemed not disclosable

must display an "Attachments Not Disclosable" page in place of the under-review notice.

PWS 5.4.4.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 51

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.3 Public Disclosure After PII Review (PWS 5.4.4.3)

STATEMENT OF WORK (PWS 5.4.4.3):

5.4.4.3 Public Disclosure After PII Review

The contractor must propose a government approved solution and implement, including but not limited to, an automated solution that discloses the redacted attachments if redacted replacing the under-review notice or actual attachments if they did not have PII data. The solution must reconcile filing received against disclosed and correct any discrepancies.

PWS 5.4.4.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 51

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.4 Revoke Public Access and Disclosure Changes (PWS 5.4.4.4)

STATEMENT OF WORK (PWS 5.4.4.4):

5.4.4.4 Revoke Public Access and Disclosure Changes

The contractor must propose and implement a solution that allows the COR or COR designee to revoke public access to any filing at any time via the web portal, upon which the solution must automatically replace the attachments with an "Attachments Not Disclosable". The system must generate a regular IRD-defined reconciliation file of Acknowledgement IDs for processed filings not yet appearing in Government disclosure files; the system must provide revisions in subsequent daily files.

PWS 5.4.4.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 51-52

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.5 Authenticated Filer Applications (PWS 5.4.4.5)

STATEMENT OF WORK (PWS 5.4.4.5):

5.4.4.5 Authenticated Filer Applications

The Contractor must implement web applications for authenticated filers to review and/or submit their filings. The application must provide the authenticated user with a summary profile of their account showing their contact information and other pertinent information.

The application must host Government-approved online instructions, help text, video(s), and other aids as needed for user exchange through these applications. The aids must reflect the difference between users that prepare a filing and users that sign a filing. The aids must stress the significance of the actions needed to submit a filing, and how users can ensure error-free filing submission.

The contractor must ensure that applications use secure communications from the beginning of the login of a user to the completion of the transaction using FIPS compliant cryptography algorithms.

PWS 5.4.4.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 52

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.6 My Filings (PWS 5.4.4.6)

STATEMENT OF WORK (PWS 5.4.4.6):

5.4.4.6 My Filings

The Contractor must implement the user-friendly My Filings web application to include the following:

- Display a summary listing of all submitted EFAST2 filings that were signed/submitted by the authenticated user, whether submitted through web application or EFAST2-approved third-party provider. Display the filing acceptance status of each submission, and a detailed list of errors. By default, this listing must be sorted in descending order of the received date time of the filings. The Form 5558 will not be displayed to users on the summary page.
- Display a summary listing all unsubmitted web filings that were created/imported by the authenticated user but have not yet been deleted by the user. Display the signature status of each unsubmitted web filing and clearly indicate to the user these have not been submitted to the Government.
- Allow the authenticated user to sort, group, and filter the displayed summary filing list(s) by filing signer, EIN, plan year, Filing Status, and/or date ranges. Allow the user to print the grouped/sorted/filtered summary filing list where the printout contains the filing information displayed on the Submissions web page of only filings matching the user- specified criteria. The user must be able to easily remove filter or group selections and revert to the default Submissions web page.
- Upon the individual's selection of a filing from the default, sorted, grouped, or filtered Submissions listing, display and allow the authenticated user to print completed or assembled filings from the summary list in a PDF facsimile format.
- Display and allow the user to print filing status information and specific errors retrieved from "Filing Acceptance Service".

Volume I - Technical Approach

- Allow an authenticated user to upload a single XML data and/or approved format-based data file filing conforming to the Filing structure defined in the DER, consisting of a Filing Header element and all forms, schedules, and attachments. After uploading the filing component, the user must be provided the ability to continue editing the filing within web application. The filing web application must automatically extract all of the individual filing components, allowing individual components to be edited and managed independently. A filing upload must not overwrite any existing filing in storage, regardless of file name duplication.
- Allow an authenticated user to download a single XML file filing conforming to the Filing structure defined in the DER, consisting of a Filing Header element and all forms, schedules, and attachments. The download feature must ensure that any signed filings that are downloaded do not contain any signature elements such that downloaded copies of signed filings are no longer considered to be a valid signed filing.
- Allow an authenticated user to copy filings from an active form year and create a new unsubmitted filing in “web-based filing application” based off an existing submitted or unsubmitted filing.
- If a submitted Form 5500 series filing is copied to the current plan/form year, it must be treated as an amendment. The Amended field on the main form must automatically be selected, all form fields and attachments must copy to the new unsubmitted filing except the signatures, and the Reference Acknowledgement ID in the new unsubmitted filing must be populated with the Acknowledgement ID of the submitted filing.
- If a submitted Form 5500 series filing is copied to the next plan/form year, only plan name, plan number, sponsor business code, plan feature codes, plan funding arrangements, and sponsor and administrator names addresses, EINs, and telephone numbers will be copied to the new filing.
- If PII is found in a filer’s submission, the authenticated filer should be able to view both the original submission and the redacted version that is publicly disclosed.

PWS 5.4.4.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 52-53

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7 Filing Web Application (PWS 5.4.4.7)**STATEMENT OF WORK (PWS 5.4.4.7):****5.4.4.7 Filing Web Application**

PWS 5.4.4.7, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 53

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7.1 Filing Creation (PWS 5.4.4.7.1)

STATEMENT OF WORK (PWS 5.4.4.7.1):**5.4.4.7.1 Filing Creation**

The Contractor must develop user-friendly web-based filing application to include the following:

- “Web-based filing application” must provide authenticated filers with a choice to either (a) select a specific valid Form Year and Form Type or (b) use an interactive style question interface to determine the correct Form Year and Form Type based upon the requirements specified in the instructions for the form.
- If a filer elects to use Filing Web Application an interactive question interface, the application must automatically populate the Plan Year Begin Date on all filer-created Form and Schedules based on the user- provided information from the form selection questions. Additionally, if the filer provides a Plan Year Begin Date of January 1st, then the Plan Year End date must default to December 31st of the corresponding year. Otherwise, the Plan Year End date must not contain a default value. The default Plan Year Begin and Plan Year End date(s) must be editable by the filer.
- Based on filer preference, automatically populate identifying information on the main form based on previous years’ filings.
- Automatically populate the EIN and Plan Number fields on the Schedules (including the MB, SB and A) from the corresponding EIN and Plan Number information provided on the main form. Filers must have the ability to modify these auto-populated fields on Schedule A only.
- Automatically populate XML elements required by schema but allowed to be blank in government instructions (e.g., Plan Year Begin Date on Form 5500).
- Allow filer data entry on any main form or schedule.
- Allow filers to upload attachments in either plain text or Adobe PDF format and include such attachments in a filing. The “web-based filing application” attachment upload function must describe the valid file types; Instruct filers that password protected files are not allowed; Alert users to the maximum length of file names; and provide/offer relevant assistance as needed. In the event a user attempts to upload an attachment that is password protected or in an invalid format, the following warning message must be displayed, "The file you attempted to attach is not a valid format or may be password protected or encrypted. Please try again." These warnings and informational messages must be clearly displayed on the webpage and must not be mouse-over tooltips.
- Convert filing data entry to government approved data format and support XML currently used in EFAST as specified in the DER.
- Allow the filer to proactively check the filing for errors using the schema validation and edit test criteria specified in the DER and notify user of errors.
- Allow a filer to upload into “web-based filing application” or download out of “web-based filing application”, unassembled filing components in XML format. For upload and download purposes, a filing component is defined as a single XML file conforming to a single child element of the filing data element structure defined in the DER, representing a single form, schedule, or attachment. No upload or download must overwrite any filing component, regardless of file name duplication. The “web-based filing application” download feature must ensure that any signed filings that are exported do not contain any signature elements such that downloaded copies of signed filings are no longer considered to be a valid signed filing. After uploading the filing component, the end user must be provided the ability to continue editing the filing component within “web-based filing application”.
- Retain work in progress of filing components, such as partially or wholly filled out components, whether complete or not, and resume editing of those stored components. The stored filings and components may be viewed/edited by the filer until deleted by the filer.
- Uniquely displaying Schedule(s) A such that repeating instances of Schedule(s) A can be easily identified

Volume I - Technical Approach

by the user. Schedule(s) A must be named using a combination the literal text “Schedule A – ” followed by the data provided on Lines 1(d) - Contract or User ID Numbers and 1(e) - Number of Persons Covered from each Schedule A.

- Allow the filer to assemble selected filing components into a single filing, resulting in a filing structure specified in the DER.
- Utilize address verification software which will validate Plan Sponsor and Plan Administrator U.S. Mailing Addresses are valid. No other addresses, including Foreign addresses, will be verified. The address verification software will be integrated in the “web-based filing application” application user interface such that upon entering the Plan Sponsor’s U.S. Mailing Address or Plan Administrator’s US Mailing Address data, the system will automatically check the address and determine if it exists and is valid. The filer will have the option to accept the system-recommended address standardization or retain user-entered data. If the Plan Administrator U.S. Mailing Address is indicated to be “Same as Plan Sponsor Address,” and the Plan Sponsor address has already been validated, the validation will not be performed again.
- Display and allow the filer to print partially or wholly completed or assembled filings in a PDF facsimile format.
- Allow for standalone schedule authoring.
- Allow the filer to manage attachments, replicate and amend filings
- Allow the filer to provide information using structure attachments rather than pdf.
- Allow the filer to create pdf of individual filing components.
- Allow for import/export of filings, schedules and attachments.
- Provide the filer with the ability to validate their filing prior to submission so filings can be submitted without errors.
- Allow the ability to link Schedule DCG using EIN and PN.

PWS 5.4.4.7.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 53-55

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7.2 Filing Signing (PWS 5.4.4.7.2)

STATEMENT OF WORK (PWS 5.4.4.7.2):

5.4.4.7.2 Filing Signing

The Contractor must maintain the user-friendly “web-based filing application” to include the below filing signing features. However, this is not required or applicable for the Form 5558 or Form PR.

- Allow multiple authorized filers to electronically review and sign a single assembled filing.
- Send filers other than the active “web-based filing application” user an email notifying them that they have a filing to sign.
- In the filing signing process, “web-based filing application” must:
 - o Display identifying filing entity information (plan name, sponsor name, EIN, plan number, and plan year end date) and a link to the filing in its entirety.

- o Automatically run a pre-validation check to determine whether the filing will be accepted by “Filing Acceptance Service”. If there are any errors or warnings identified in the pre-validation check, allow the user to (1) fix the errors or (2) continue to sign the filing.
- o Present the user with a Government-approved signature agreement.
- o Allow the user to specify which line/role they are affixing their signature onto. The DFE signer line/role must only be available for Form 5500 filings, not 5500-SF or 5500-EZ.
 - Automatically rewrite the Filing Header each time the filing is signed and apply signer’s name and signing date to the form.
 - Disallow the Filing Header to be accessed directly or edited and must automatically erase all signatures in the Filing Header if an assembled filing is edited after signing.

PWS 5.4.4.7.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 55

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7.3 Filing Submission (PWS 5.4.4.7.3)

STATEMENT OF WORK (PWS 5.4.4.7.3):

5.4.4.7.3 Filing Submission

The Contractor must maintain the user-friendly “web-based filing application” to include the following:

- Allow users to electronically submit the assembled filing and transmit it to “Filing Acceptance Service” using the required web service protocols and message formats and receive receipt and acknowledgment.
- Allow users to validate their submission so they have an opportunity to correct the filing prior to submission.

PWS 5.4.4.7.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 55-56

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7.4 Form PR (PWS 5.4.4.7.4)

STATEMENT OF WORK (PWS 5.4.4.7.4):

5.4.4.7.4 Form PR

The Contractor must develop the user-friendly “web-based filing application” to include support for the Form PR (Pooled Plan Provider Registration form) in accordance with the SECURE Act. Pooled Plan Provider registration is a one-time event for providers, unless changes to the terms of the pooled plan occur (which may require filing amendments). A webservice for this form is not needed for third party

developers. Filers leverage EFAST2 accounts for Form PR submission and to review the status of registration progress and submissions. The Contractor must allow the public users to search Form PR statements based on filer contact information or filing entity information and as defined in the EFAST2 system. The contractor must also allow users to download the Form PR data through government approved APIs and data formats.

PWS 5.4.4.7.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 56

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.4.7.5 Authenticated Government Functions (PWS 5.4.4.7.5)

STATEMENT OF WORK (PWS 5.4.4.7.5):

5.4.4.7.5 Authenticated Government Functions

In addition to monitoring access specified in other sections, the Contractor must provide the following web-based functions specific to Government users.

5.4.4.7.5.1 Filing Display

- The Contractor must operate and maintain a web-based function or application for authenticated Contractor and Government users to review filings and Form PR statements.
- The Contractor must authenticate users based on their Government-issued HSPD-12 PIV access cards.
- The Contractor must allow the user to search for filings or Form PR statements based on filer contact information or filing entity information.
- The Contractor must provide real-time matching results of all submitted EFAST2 filings and Form PR statements that were signed/submitted, whether submitted through “web-based filing application” or EFAST2-approved third-party provider. The application must display the filing acceptance status of each filing submission based on the Filing Status Response data, and a detailed list of errors. By default, this listing must be sorted in descending order of the received data and time of the filing. The PDF facsimiles available to authenticated Government users must include all elements of the Processed Filing data.
- The Contractor must provide real-time matching results of all unsubmitted “web-based filing application” filings and Form PR statements that were created/imported but have not yet been deleted by the user. The application must display the signature status of each unsubmitted “web-based filing application” filing and Form PR statement and clearly indicate these have not been submitted to the Government.
- The Contractor should leverage components of the My Filings application or the public search application for efficiency.
- The Contractor should leverage or interface Contact Center applications to the Filing Display function/application.

5.4.4.7.5.2 Secure/Substitute Filing

The Contractor must operate and maintain the “web-based filing application” such that an authenticated Government user may submit a secure/substitute Form 5500 series filing. Secured/substitute filings are subject to schema validation and authentication of Government signer’s credentials. Secured/substitute filing submissions must bypass edit testing through the assignment of a Bypass Code as defined in the

DER.

5.4.4.7.5.3 Revoking Access to Filings

The Contractor must establish a means to facilitate the granting and revoking of access permissions to specific filings or filing attachments by the COR or COR designee.

PWS 5.4.4.7.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 56-57

THIS PARAGRAPH HAS THREE NUMBERED SUBPARAGRAPHS. ANSWER ALL THREE.

PWS 5.4.4.7.5 contains 5.4.4.7.5.1 Filing Display, 5.4.4.7.5.2 Secure/Substitute Filing and 5.4.4.7.5.3 Revoking Access to Filings. All three are quoted in full in the box above.

They are six levels deep. The company template's multilevel numbering stops at Heading 5, so they cannot carry their own numbered headings without adding a style, which is not permitted. Answer each by name inside this section, and list all three in the cross-reference matrix that Instructions E requires so the traceability is explicit.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5 Artificial Intelligence (AI)-Enabled Development, Modernization, and Enhancement (DME) (PWS 5.4.5)

STATEMENT OF WORK (PWS 5.4.5):

5.4.5 Artificial Intelligence (AI)-Enabled Development, Modernization, and Enhancement (DME)

Maximize the practical use of Artificial Intelligence (AI), including machine learning (ML), automation, and generative AI, to accelerate DME activities, reduce time to delivery, improve quality, and lower cost while maintaining or improving security, privacy, accessibility, equity, and overall mission outcomes. The Contractor must be compliant with all AI clauses supplied by DOL, as issued and updated by the Department, in addition to the specific requirements set forth in this section.

PWS 5.4.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 57

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5.1 Proactive use of AI (PWS 5.4.5.1)

STATEMENT OF WORK (PWS 5.4.5.1):

5.4.5.1 Proactive use of AI

- The Contractor must identify, propose, and employ AI capabilities wherever practicable and beneficial to DME tasks (e.g., code and test generation, refactoring, documentation, infrastructure-as-code, test data synthesis using de-identified data, CI/CD and AIOps automation, requirements/user-story refinement), provided such use complies with applicable laws, regulations, and agency policies.
- AI must not be used to perform inherently governmental functions and must not replace required human determinations; AI outputs must be treated as draft and are subject to human review and acceptance by qualified personnel.

PWS 5.4.5.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 57

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5.2 Transparency and prior notification (PWS 5.4.5.2)**STATEMENT OF WORK (PWS 5.4.5.2):****5.4.5.2 Transparency and prior notification**

- The Contractor must submit an AI Enablement Plan describing the AI tools and services to be used, DME use cases, expected benefits with quantitative targets, measurement methods, data sources and handling, human oversight, testing/validation approach, risk management, licensing/IP, and rollback criteria.

PWS 5.4.5.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 57-58

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5.3 Security, privacy, and data handling (PWS 5.4.5.3)**STATEMENT OF WORK (PWS 5.4.5.3):****5.4.5.3 Security, privacy, and data handling**

- The Contractor must not input, upload, or expose non-public Government information (e.g., CUI, PII, PHI, FTI, SSI, procurement-sensitive information, or non-public source code) to external/public AI services or allow Government data to be used for provider model training unless explicitly authorized in writing by the Government and protected by approved contractual and technical safeguards (e.g., Government-tenant, data isolation, no-retention/no-training clauses).
- Any AI capability used for DME must operate within environments that meet applicable security and privacy requirements (e.g., FedRAMP for cloud services; NIST, agency cybersecurity baselines; records management; Section 508; plain language). The Contractor must maintain prompt/output and model/tool

usage logs consistent with agency policy and provide them upon request.

- Any fine-tuning or model customization using Government-furnished data requires prior written authorization and must occur in a Government-approved environment with documented controls. The Contractor must ensure that no licensing terms permit reuse of Government data or outputs outside the scope of this contract.

PWS 5.4.5.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 58

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5.4 Quality and compliance (PWS 5.4.5.5)

STATEMENT OF WORK (PWS 5.4.5.5):

5.4.5.5 Quality and compliance

- AI-assisted code, configurations, and documentation are subject to the same acceptance criteria, quality standards, and security testing (e.g., SAST/DAST/IAST, dependency and license scanning) as manually produced artifacts. The Contractor remains accountable for correctness, quality, accessibility, and security of all deliverables.
- The Contractor must apply an AI risk management approach aligned to current Federal guidance (e.g., OMB policy and the NIST AI Risk Management Framework), including bias, safety, explainability, and performance considerations commensurate with impact. Any AI that interacts with end users or could materially affect individuals or mission outcomes requires an impact assessment and Government concurrence prior to use.

PWS 5.4.5.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 58

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.4.5.5 Intellectual property and deliverables (PWS 5.4.5.6)

STATEMENT OF WORK (PWS 5.4.5.6):

5.4.5.6 Intellectual property and deliverables

- AI-generated or AI-assisted artifacts (e.g., code, test cases, documentation, models developed under the contract) are contract deliverables and subject to the same data and intellectual property rights as other deliverables under this contract.

PWS 5.4.5.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 58

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.5 Direct User Exchange (PWS 5.5)

STATEMENT OF WORK (PWS 5.5):

5.5 Direct User Exchange

- The branding, style, terminology, and user interface of EFAST2 must seamlessly flow and be part of the Contractor's overall EFAST2 user exchange (UX) design. This includes the EFAST2 website, public documentation/aids, and contact center.
- The Contractor's user exchange must be intuitive and in the standard English language.
- The Contractor must define UX goals and tasks and then ensure interfaces provide affordance, comprehensibility, responsive feedback, explorability, forgiveness, efficiency, and predictability. The Contractor must strive for the simplest designs by focusing on what is probable and reducing/hiding what is unlikely. Probable tasks must require minimal effort for users to perform. The Contractor must design points of user exchange with the goal that users should not need to interact with a live agent.
- The Contractor must establish UX review and clearance processes that ensure public content (User Guides, tutorials, FAQ's) is appropriately reviewed and cleared prior to release. Public content must be 508 compliant. Changes must be made available in CAT for the Government's approval prior to release into production in accordance with Government- approved procedures.
- Typical UX changes requested by the Government will be non-urgent. Occasionally the Government may request urgent UX changes specific to content.
- The Contractor must document and implement a formal process of periodic UX audits and updates. The audits must check that all information is current and accurate, make new information available, and check that all links are still operational.
- The Contractor must document and maintain user stories or use cases or similar documentation illustrating stakeholder user exchanges with EFAST2.

PWS 5.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 58-59

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.5.1 Website (PWS 5.5.1)

STATEMENT OF WORK (PWS 5.5.1):

5.5.1 Website The Contractor must operate and maintain a user-friendly (as defined by such authorities on usability and accessibility as <http://usability.gov> and <http://www.w3.org/>) EFAST2 website. The website

Volume I - Technical Approach

must provide a central location for filers to directly access EFAST2 applications, services, and information. The website must be exclusively on the Government-provided domain. The Contractor must define and coordinate with the Government procedures and timelines for any DNS and MX cutovers or changes.

The website must account for both experienced and novice computer users. The Contractor must promote:

- The use of plain language, in accordance with the Plain Writing Act of 2010;
- The use of responsive web design in accordance with the Digital Government Strategy;
- “Anywhere, anytime, on any device” (e.g. using HTML5 and CSS3);
- Best practices for structuring and tagging content (metadata and keywords) and data for search engine optimization and machine-readability;
- Effective content lifecycle management to eliminate outdated content, not defined as archival;
- Next-generation open web development, including use of content delivery networks; content management systems; common code libraries, frameworks, and tools;
- Leverage and use URL shortening in lieu of new domain requests; and
- Use of industry best practices for “Smarter IT delivery” as defined by the CIO Playbook.
- The website must adhere to:
 - OMB Policies for Federal Public Websites
 - U.S. Web Design System principles and guidelines
 - NIST publication 800-44 Guidelines on Securing Public Web Servers
 - E-Government Act of 2002
 - DOL Web Community Standards for Design, Navigation, and Cross-Functionality with regard to the standard terminology, color palette & typography, standard page elements, visual hierarchy, and global navigation and cross-functionality.

In efforts to allow the General Services Administration (GSA) to gather web metrics across the Federal Government for its Digital Analytics Program, the Contractor must implement the Google Analytics code on production EFAST2 static web pages. The Google Analytics code is intended to coexist with EFAST2 metrics and is not intended as a substitute for other metrics necessary to support the Contractor's operational monitoring.

All pages on the website must provide users with:

- Self-service features that allow users to complete actions and obtain information easily, minimizing the need to call the EFAST2 Contact Center.
- Customized assistance to users regarding completing, signing, and submitting filings, and dealing with filing errors.
- An integrated search function
- The most current information and resources available for EFAST2 filers, including a detailed list of EFAST2-approved third-party software
- Government-approved links to websites outside of the EFAST2 subdomain.

The website must link to the Contact Center application and Contact Center application functionality, allowing users to send questions electronically via email or web-form.

The Contractor must consider the speed of user connections and the general levels of travel on the web

Volume I - Technical Approach

when planning and implementing the portal. The portal must use compressed graphics formats, such as GIF, PNG or JPEG to reduce download or access time. For files, the portal must provide information on the size of the file and allow users the option to download if they so choose.

PWS 5.5.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 59-60

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.5.2 Compatibility and Accessibility (PWS 5.5.2)

STATEMENT OF WORK (PWS 5.5.2):

5.5.2 Compatibility and Accessibility The web portal must be compatible with wide ranges of configurations. All pages must be viewable on Microsoft Windows and Apple Macintosh platforms without the page layout or functionality changing significantly.

It is the Contractor's responsibility to ensure compliance with the most current web browsers throughout the contract life cycle. All pages of the web portal must be viewable by, at a minimum, the top three Internet browsers according to the Digital Analytics Program (reference <https://analytics.usa.gov/>). The portal must maintain compatibility with the current version and at least one older version of each browser. As new browsers and versions become available, the portal must be proactively tested against beta versions.

Web based viewing, searching, and access applications from the EFAST2 Web portal, and data dissemination systems must not require the user to download any software, driver, plug-in, control or browser extension in order to successfully use application features. The Contractor is permitted to require the user to have or download and install a PDF viewer for filing and facsimile viewing. Formats must be limited to HTML,

XML, JPG, GIF, PNG, PDF and safe JavaScript. The web methodology must also be designed not to require bypass of required firewall and proxy server features. The Website Design, web file formats, and web methodology are subject to Government inspection and acceptance and security evaluation. The EFAST2 website (content, documents, PDF's and files) must meet all requirements from Section 508 of the Rehabilitation Act (29 U.S.C. 794d). Section 508 requires federal agencies to ensure that their procurement of information technology takes into account the needs of all users, including those with disabilities. The Contractor must conduct quarterly application testing and application updates (if applicable) to ensure ongoing Section 508 compliance and compatibility with browser support requirements.

Except for meeting the requirements from Section 508 of the Rehabilitation Act (29 U.S.C. 794d) and other needs of users with disabilities, horizontal scrolling must be minimized wherever possible when the width of the browser is set to a standard size of 800x600. All page images must fit into the standard screen width. The use of vertical scrolling is acceptable but should also be minimized.

PWS 5.5.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 60-61

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.5.3 Cookies and Session Data (PWS 5.5.3)

STATEMENT OF WORK (PWS 5.5.3):

5.5.3 Cookies and Session Data In order to provide stateful storage of information, cookies or other session mechanisms may be used in accordance with DOL policies.

PWS 5.5.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 61

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.6 Data Dissemination (PWS 5.6)

STATEMENT OF WORK (PWS 5.6):

5.6 Data Dissemination

The Contractor must create output records of filing data suitable for dissemination to Government end users and public disclosure in accordance with the IRD. Output Records must be retained for all years.

PWS 5.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 61

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.7 Reports (PWS 5.7)

STATEMENT OF WORK (PWS 5.7):

5.7 Reports

The Contractor must implement reports for government users as per the requirements. To assist the Government in monitoring year-to-year continuity of large plan filings, the Contractor must provide a Large Plan Report via a web-based interface which can be accessed at any time by the Government. The Large Plan Report must show the current status of all filing submissions for fifty of the largest defined benefit plans. The plans serving as the basis for the initial report will be identified by the Government as GFI. This report must indicate the following fields from the database such as EIN, PN, SPONSOR NAME, PLAN NAME, PLAN DATES, Duplicate Indicator, Amendment Identification, and Filing Status.

Volume I - Technical Approach

The report must also include explanatory comments if needed, such as those provided by the data management coordinator. There may be multiple entries in the report for a single plan. The report must be grouped by EIN and PN. The report must be updated no less than daily and show all filing records for the identified plans. Additionally, each year when a new form version is incorporated into the system with the annual rollover, the report must include the EIN and PN for all identified plans. The initial filing status of the new form version filings will be "Not Yet Received". Once the corresponding filing record is received and processed by the system, the report must be updated to reflect the required information from the Tracking Database. All other reports currently present in EFAST must be modernized based on the existing and new requirements from government.

PWS 5.7, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 61-62

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.8 Contact Center (PWS 5.8)

STATEMENT OF WORK (PWS 5.8):

5.8 Contact Center

The Contractor must implement tools to support the Contact Center that are accessible to all inquirers. The Contact Center must be aligned with the branding, style, terminology, and interface of the overall EFAST2 user exchange (UX) design, as described in the Direct User Exchange Section above.

The Contractor must record all inquiries into and Contractor responses through the Contact Center. The Contractor must provide DOL agency stakeholders with the ability to access live and recorded inquiries remotely. Both recorded and live inquiries must be available and used for Contractor and Government monitoring. The Contractor should provide callers with an estimated wait time in queue. When providing an estimated wait time in queue, caller should be provided the option of leaving a voicemail or being called back as described in the next paragraph.

The Contractor should implement virtual call queuing technology allowing callers to choose to receive a live callback when they reach the front of the queue, as opposed to waiting on hold to be connected to a live operator. This virtual hold must be counted the same as waiting on hold when calculating performance standards. Callback should take into account caller's time zone when placing call, as well as provide the caller the ability to specify an alternate callback number and/or date/time. If a live operator is not available at the Government agency, the Contractor must leave a voice message with the Government agency specifying the nature of the call, service ticket number, and inquirer's name and phone number.

The Contractor must implement a tool to support voice response system to queue, manage, and triage calls to the Contact Center. The Contractor must maintain the personas, user journeys, and conversation flows. Conversations must be guided with probable multiple-choice options and not reach a dead end. Routine inquiries should be addressed via the programmed options to minimize the number of calls requiring live operator assistance. However, should the system be unable to adequately address a caller's need, the Contractor must provide a means for the caller to reach a Contact Center representative by simply entering "0" or similar code. Trends in caller menu selections should be analyzed to ensure that routine inquiries continue to be addressed via the options. This journey must be logged against a relevant service ticket and,

Volume I - Technical Approach

if ultimately answered by an agent, the agent should be informed of the journey taken.

The Contractor must establish a voice mailbox to provide callers with an option to leave a message after the established hours of operation.

The Contractor must handle and respond to electronic correspondence (e.g., email/webchat) received by the Contact Center in accordance with the procedures defined below. That action will include one of the following:

- Providing the user with a Government pre-approved response or a link to existing information on the public web site.
- Developing and sending a response which addresses the issues of the correspondence in the event the correspondent is authorized by the Government to respond to those issues.
- Forwarding the correspondence to another Government mailbox designated to respond to public correspondence for action (with a notification of the action sent to the inquirer).
- Determining a response is required but additional time is needed to prepare the response (with a notification of the determination sent to the inquirer).
- Determining that no response is required.
- Logging this interaction into the appropriate service ticket.

The Contractor will establish and maintain approved Internet Correspondents. All electronic responses, or electronically forwarded messages, must contain the Internet Correspondent's name or a unique identification code in order to maintain an audit trail, such as the acronym EFAST followed by a three-digit number (e.g., EFAST-001).

PWS 5.8, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 62-63

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.8.1 Written Inquiries (PWS 5.8.1)

STATEMENT OF WORK (PWS 5.8.1):

5.8.1 Written Inquiries Internet Correspondents may respond only to subject matter and/or other types of correspondence consistent with the EFAST2 program and for which they have been granted response authority. An Internet Correspondent who receives correspondence requiring a response that is beyond the scope of authority granted to the Internet Correspondent will forward the correspondence to the appropriate Government agency.

Internet Correspondents should respond to electronic correspondence via the same method that the request was received. If the nature of an electronic inquiry is such that it would require a formal response signed by an agency official if it were received by mail, then the response must be transferred to the appropriate Government agency.

The Contractor must attach a disclaimer to all responses that require an interpretation of statute, regulation, or filing instructions, unless the response has been vetted through an official departmental and/or agency clearance process, such as an FAQ or DOL/agency Web page. The disclaimer should read: "This response

is for information purposes only and does not constitute an official interpretation of the U.S. Government." The Contractor should include the disclaimer if there is any doubt about whether it is necessary.

All written correspondence must be stored and retained for the life of the contract in a format enabling basic searches and retrieval of email and consistent with regulations and requirements of the National Archives and Records Administration (NARA). All email and webchat correspondence must be furnished to the Government upon Government request. All activities related to email and web chat correspondence must be handled in accordance with 36 CFR 1234, Electronic Records Management.

PWS 5.8.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 63

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.8.2 Chatbot/AI Solution (PWS 5.8.2)

STATEMENT OF WORK (PWS 5.8.2):

5.8.2 Chatbot/AI Solution The Contractor may use AI based solution/chatbot(s) for improved efficiency and customer experience. All solutions must provide trustworthy, accurate, relevant, and reliable responses to caller questions. The software architecture should be designed in a way that appropriate parts may be reused in the future.

The Contractor must interface the solution with live agent support such that a live agent can take over conversations when alerted by the bot.

Users should be able to ask questions and get definitive answers in the format of a one-to-one conversation on real time basis.

The chatbot should:

- Take user inputs (keywords/buttons) from close-ended queries and respond in conversational language
- Reconfirm the query in mutually understandable language in case of complex natural language queries
- Find matching answers from the Government-approved knowledge base.
- Accurately match answers to questions

If the chat fails to understand a query, it should offer closely matching questions as options for the users to choose from, along with a NOTA ('none of the above' option). If a user chooses NOTA, or, the chatbot fails to find matching information, the chatbot should:

- Provide an appropriate website link where the user could look for the answer, and check if the webpage resolved the query.
- If the call is during business hours, alert a human agent and let him/her take over the conversation via a digital interface.
- If the call is not during business hours, take a message that will be returned by a human agent.

In case of loss of connectivity, the bot should be able to resend the missed messages or resume the

Volume I - Technical Approach

conversation within the on-going flow when connectivity is restored.

Trends in chatbot interactions (specifically accuracy, responsiveness, opt-out, NOTA must be analyzed to ensure that the same level of customer experience is maintained via the Chatbot option as if the inquiry were routed to a human agent.

Trends in caller menu selections must be analyzed to ensure that routine inquiries continue to be addressed via the options. This journey must be logged against a relevant service ticket and, if ultimately answered by an agent, the agent should be informed of the journey taken. The Contractor must use a service ticket application, such as a customer relationship management (CRM) solution, to track and report inquiries made to the Contact Center.

The application must store and generate reports of information regarding a description of the inquiry, inquirer contact information, servicing agent, status of inquiry (open, closed, etc.), categories for reporting, and inquiry

age. The application must allow for Contractor-defined service codes, resolution codes, and cause codes. The application must be capable of allowing the assignment of specific fields to be mandatory fields. For example, the contact information (name, phone number) may be mandatory fields on the service ticket application screen.

Service ticket information must be maintained throughout the duration of the contract and must be accessible by a number of criteria, such as telephone number, name of person who called, etc. Service ticket history must be tied to both the person having the problem (i.e., the plan administrator) as well as the person calling in the trouble (i.e., the preparer).

The service ticket application must provide an integrated, automated service reporting mechanism that assigns service tickets to Contractor staff. The application must allow non-Contact Center personnel (i.e., the Contractor's data management analysts, authorized Government staff, etc.) to append to service tickets as appropriate.

The application must provide a method for prompting the Contact Center staff member through the steps of receiving and documenting a service ticket, including service specific trouble-shooting procedures. These steps must prompt the Contact Center staff to ask a series of trouble-shooting questions (are you connected to the internet, can you get to the home page, etc.) during the inquiry session. The application must have the capability of accepting up to 10,000 service tickets per day.

The application must allow written notification to be sent to the person who submitted the inquiry. This notification could include receipt of the service ticket, assignment of the service ticket, and completion of the service ticket.

The application must automatically assign a unique identification number for each service ticket created. Ticket numbers must be used by the Contractor to track and reference inquiries. The ticket number is to be assigned upon initial inquiry. The Contractor must provide the Government with access to the Service Ticket system and reports.

The Contractor must provide the Government with a web-based interface to monitor reports of near-real time Contact Center operations.

The application must, without prompting the human agent, provide notification if a previous service ticket exists for the caller and/or the issue the caller is calling about.

The application must allow the reporting on service tickets to determine how many contacts, what type of contact (inbound voice, outbound voice, inbound E-Mail, outbound E-Mail, inbound Chat, Voicemail, Chatbot) and time between each contact in an effort to better understand interactions not resolved in the first contact.

The Contractor must analyze the service tickets to identify patterns indicating recurrent issues and, if a

Volume I - Technical Approach

recurrent issue is identified, take action, by notifying the Government agency or taking action internally, work around the recurrent issue or identify and implement a solution to the root cause of the recurrent issue.

The Contractor must provide the Government with agreed upon quantitative reports of inquiries, concurrencies, holds, abandonments, response times, ratios, survey responses, and other data in time increments and detail agreed upon by the Government.

PWS 5.8.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 63-66

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.8.3 Release Notes (PWS 5.8.3)**STATEMENT OF WORK (PWS 5.8.3):**

5.8.3 Release Notes On the day of the production deployment, the contractor must notify the Government of the production releases with summary of features released and known defects from the release and work around for the defect if applicable.

PWS 5.8.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 66

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.9 Data Management and Migration (PWS 5.9)**STATEMENT OF WORK (PWS 5.9):****5.9 Data Management and Migration**

The Contractor must maintain the following specified data repositories as well as other data repositories as necessary to implement the requirements of this PWS. All data repositories must be made available for querying for data management monitoring purposes.

The Contractor's evaluation must integrate the various system reports and use meta-analysis to research and comprehend potential problems. The Contractor must use monitoring tools and procedures to identify potential problems in data management, troubleshoot the problems to determine the root cause of the problems, and identify needed fixes. Information on data management problems, bottlenecks, or delays, particularly recurring ones, must be made available to the Government. Form 5558 data must be stored in a repository in accordance with applicable safeguarding standards for FTI. This includes adherence to applicable requirements detailed in IRS Publication 1075 (with the exception of the Safeguards Security Report (SSR) and implementation of IAL-1, which are not required for this effort). Any FTI safeguarding

Volume I - Technical Approach

requirements that cannot be met must be clearly documented and submitted to the Government for review and approval to include mitigation recommendations as detailed by the Cyber Security process.

The Contractor must create selected record sets (XML and Structured data) for distribution to the Government. Distribution files must be pushed to DOL, IRS, and PBGC as required by Government-issued Interface Requirements Document (IRD). The IRD provides specificity on the exact data that should be sent to each agency. The Deliverable schedule (Technical Exhibit 2) provides the frequency and number of files to be pushed to each agency. Pushing the files will involve connecting to the Government secure drop box servers through the Internet, securely transferring files to a specified directory, then renaming the files in the directory. The Contractor must ensure each pushed file is a reasonable file size for uploading and downloading. If necessary, the Contractor must create multiple files for each drop box to ensure no file sizes are unreasonably large. After the required files have been pushed to an agency, the Contractor must transmit an e-mail notification to that agency's contact notifying them that their files are ready for pickup.

The contractor must import and incorporate legacy EFAST2 data from the database, documents and contact center data, files and any EFAST2 related files into the modernized system by production release.

PWS 5.9, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 66-67

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.10 Testing and Deployment (PWS 5.10)

STATEMENT OF WORK (PWS 5.10):

5.10 Testing and Deployment

The contractor must provide testing and deployment services with a focus on end-to-end automated testing include unit testing, functional testing, regression testing, performance testing, load testing, post-production testing and product deployment. Key Goals:

- Product performance tested and ready for public go-live.
- Data transfers to external entities operational.
- All production data validated.
- Product training developed.
- Product soft launched.
- Product go-live.

Deliverables:

- Final fully functioning product available for the American public to use. Performance

Metrics:

- Usage metrics from CSAT tools.

PWS 5.10, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 67

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.11 DevSecOps (PWS 5.11)

STATEMENT OF WORK (PWS 5.11):

5.11 DevSecOps

The Contractor's DevSecOps practices will automate testing and code/deployment promotion. The Contractor's code pipeline will be based on containers and version control.

The contractor must conduct and execute Sprint cycles which must include requirements definition and prioritization, design specification, and a development and operational testing cycle. The contractor must bundle the two-week sprint cycles into monthly production releases containing 2 sprints, unless otherwise approved in writing by the FPM.

The Contractor must ensure that Cybersecurity is fully integrated into all phases of the software development process, including initial design, development, testing, and is part of the approval process. The Contractor must ensure the proper Contractor support staff is available to participate in security test & evaluation and security authorization processes. This includes, but is not limited to:

- Attending and supporting security meetings with the Government
- Supporting/conducting the vulnerability mitigation process
- Supporting the Assessment Team during system security testing
- Defining the security authorization boundary
- Correcting or adequately mitigating security vulnerabilities
- Documenting configuration baselines

The Contractor's Detailed System Design documentation must:

- Describe its DevSecOps processes and environments.
- Address the Ports, Protocols, and Services (PPS) proposed to be used to transport data and communicate between systems.
- Identify all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface
- Identify user roles required for access control and the access privileges assigned to each role
- Address unique security requirements (e.g., encryption of key data elements at rest)
- Identify categories of sensitive information processed or stored by the application, and their specific protection plans (e.g., Privacy Act, HIPAA)
- Contain or point to a current and comprehensive baseline inventory of all software and services supporting the system (to include manufacturer, type, and version and installation manuals and procedures)
- Illustrate how all user interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems).

PWS 5.11, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 67-68

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.12 Release Management (PWS 5.12)

STATEMENT OF WORK (PWS 5.12):

5.12 Release Management

The contractor must provide Release Management support for the planning, preparation, scheduling, delivery, review, and testing of all system software releases and their supporting documentation. The contractor's approach must reflect DOL's release management process. The contractor must plan for system releases as directed and approved by the Federal Project Manager. The contractor must coordinate with appropriate development, testing, and support contractors and advise the Federal Project Manager frequently on the status of planned releases.

1. In addition to testing each Sprint Cycle and in preparation for the Production Releases, the Contractor must coordinate and perform the following test activities:

- a. Unit Testing
- b. System Integration Testing
- c. Performance/Load Testing
- d. 508 Compliance Testing
- e. Regression Testing
- f. User Acceptance Testing (UAT) – Facilitate and Assist
- g. Develop test scenarios/cases for use during UAT
- h. Schedule UAT kickoff sessions (up to 3 UAT sessions per release)
- i. Provide user support during UAT

2. The Contractor must provide test scripts and data to conduct sprint reviews and UAT with stakeholders.

3. The Contractor must modify and regression test code to resolve errors found during UAT to ensure the system is ready for production deployment. All changes must be documented in the DOL OCIO's change control/configuration management tools.

4. The Contractor must ensure that Contractor personnel providing support are DHS Trusted Tester or have an equivalency of the knowledge, skills, and ability necessary to address the applicable Revised Section 508 Standards defined in the requirement and must provide conformant Section 508 supporting documentation upon request.

5. The Contractor must document the test results and then upload the results to the project repository (e.g., DOL SharePoint). Note: Automated testing processes must be used whenever possible.

6. Two weeks Agile Sprint Cycles (unless otherwise directed by the FedPM)

7. The Contractor must conduct bi-weekly sprint reviews that consist of the following:

a. Presentations (in PowerPoint) and demonstrations (if applicable) of what has been ‘done’ during the sprint cycle, along with the number of points / velocity. The definition of ‘done’ will be defined during Sprint 0 and follow-on Sprints by the FedPM or Product Owner. I. Lessons learned (i.e., sprint retrospective) from the sprint must be part of the sprint review presentation.

II. Plans for the next sprint cycle per feedback from the PM must be part of the sprint review presentation.

III. Draft versions of (living) documentation (e.g., Design Specification, Requirements, Test Summary Report and Test Results) that have been updated as a result of the sprint must be delivered prior to the sprint review and noted in the sprint review presentation.

IV. Plan, implement, and facilitate Sprint User Acceptance Testing (UAT) sessions to allow users to test the functionalities/features of the user stories that were developed during the Sprint cycles.

PWS 5.12, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 68-69

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13 Operations and Maintenance (O&M) (PWS 5.13)

STATEMENT OF WORK (PWS 5.13):

5.13 Operations and Maintenance (O&M)

- The Contractor must operate, maintain, and continuously improve the modernized EFAST2 solution and all supporting environments and services developed under this PWS. O&M must cover the production system, pre-production/staging, test, development, and the Participant Acceptance Test System (PATS), as well as shared services and integrations (e.g., Login.gov, email services, virus scanning, address validation), databases, data pipelines, storage, logging/monitoring, and infrastructure components. All O&M activities must comply with applicable Federal and Department of Labor (DOL) policies and standards, including but not limited to FISMA, NIST SP 800-53, NIST SP 800-37, NIST SP 800-63, FIPS-validated cryptography, IRS Publication 1075 for FTL, applicable OMB memoranda, and agency security and privacy policies. Provide Operations and Maintenance (O&M) support to sustain the availability, performance, security, and reliability of system, while implementing Government-approved minor system improvements that enhance usability and operational efficiency within the current system architecture.

PWS 5.13, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 69-70

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.1 Operations (PWS 5.13.1)**STATEMENT OF WORK (PWS 5.13.1):****5.13.1 Operations**

- Operate the modernized solution to support registration, filing acceptance and processing, web-based filing applications, authenticated Government functions, public disclosure functions, and associated APIs/services.
- Provide capacity planning, auto-scaling, and performance tuning to meet peak filing periods and annual rollover needs without service degradation.
- Manage routine operational jobs (e.g., email notifications, file processing, data indexing, search updates, archival, disclosure state updates) with runbooks and automated recovery.
- Administer environments, accounts, roles, and keys in accordance with least privilege and separation of duties, with FIPS-validated cryptographic modules for data in transit and at rest.
- Maintain current, version-controlled as-built documentation, system runbooks, and Standard Operating Procedures (SOPs).

PWS 5.13.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 70

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.2 Maintenance and Release/Change Management (PWS 5.13.2)**STATEMENT OF WORK (PWS 5.13.2):****5.13.2 Maintenance and Release/Change Management:**

- Perform preventive and corrective maintenance, including patching of operating systems, middleware, databases, and application components, consistent with CISA/DOL timelines for critical/high vulnerabilities and agency-approved maintenance windows.
- Maintain CI/CD pipelines that support secure, automated deployments with rollback and blue/green or canary strategies to minimize downtime.
- Implement ITIL-aligned change management with a Government-approved Change Control Board (CCB), including impact assessments, back-out plans, and post-implementation reviews.
- Plan and execute the annual form-year rollover and DER/schema/edit test updates, coordinating with stakeholders and third-party software developers; ensure pre-production validation prior to production deployment.
- Maintain compatibility and integration with Login.gov at the Government-determined IAL and AAL levels; update integrations as service interfaces evolve.

PWS 5.13.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 70

Volume I - Technical Approach

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.3 Security, Privacy, and Compliance (Continuous ATO) (PWS 5.13.3)**STATEMENT OF WORK (PWS 5.13.3):****5.13.3 Security, Privacy, and Compliance (Continuous ATO)**

- Maintain the Authority to Operate (ATO) through continuous monitoring; produce and update security artifacts (e.g., SSP, SAR, POA&Ms, contingency plan, incident response plan, inventory, data flow diagrams) as required by RMF and DOL policy.
- Enforce identity, credential, and access management consistent with NIST SP 800-63 (IAL-1 and AAL2), and Government direction; safeguard PINs and signature elements.
- Protect PII and FTI in accordance with NIST controls and IRS Pub 1075, including logical segmentation, encryption, auditing, background checks where required, and restricted access/handling procedures.
- Perform and document routine vulnerability scanning, SAST/DAST, dependency and container image scanning, configuration compliance, and supply-chain risk management (including SBOMs and signed attestations, where required), remediating findings in accordance with DOL and CISA timelines.
- Maintain logging, audit, and centralized monitoring consistent with OMB logging requirements and agency policies; retain logs for agency-mandated periods and make them available for investigations and eDiscovery.
- Support annual tests/exercises for contingency, incident response, and privacy; update PIAs and any SORN-related documentation as directed by the Government.

PWS 5.13.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 70-71

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.4 Monitoring, Incident, and Problem Management (PWS 5.13.4)**STATEMENT OF WORK (PWS 5.13.4):****5.13.4 Monitoring, Incident, and Problem Management**

- Provide real-time monitoring and alerting for availability, latency, throughput, error rates, job failures, and security events across applications and infrastructure.
- Triage, communicate, and resolve incidents according to Government-approved severity definitions and timelines; notify the COR (and CISA/US-CERT where required) of reportable incidents within mandated timeframes.
- Conduct root cause analysis for P1/P2 incidents and recurring problems; track corrective and preventive actions to closure; update runbooks and monitoring to prevent recurrence.

PWS 5.13.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 71

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.5 Data Management, Backup, and Continuity (PWS 5.13.5)

STATEMENT OF WORK (PWS 5.13.5):

5.13.5 Data Management, Backup, and Continuity

- Implement Government-approved data retention, archival, and purge routines for filings, attachments, operational logs, and metadata aligned to records schedules, FOIA/Privacy requirements, and legal hold processes.
- Perform secure, automated, and regularly tested backups for all critical data and configurations; implement encryption for backups and secure offsite storage where required.
- Maintain and annually test a Government-approved Disaster Recovery/Continuity of Operations (DR/COOP) plan that meets defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO); document and remediate gaps.
- Ensure integrity of public disclosure workflows (e.g., “Attachments Under Review,” unhide/revocation flows) and reconcile disclosure status with Government-provided lists; re-index and republish data as directed.

PWS 5.13.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 71

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.6 Environment Stewardship and Tools (PWS 5.13.6)

STATEMENT OF WORK (PWS 5.13.6):

5.13.6 Environment Stewardship and Tools

- Maintain development, test, staging, PATS, and production environments with consistent baselines and security hardening; ensure test data is non-production and free of live PII/FTI, unless explicitly authorized and protected per policy.
- Maintain the PATS environment to mirror production validations as closely as practicable for third-party testing and certification; update PATS annually or as required for schema/business rule changes.
- Manage licenses, certificates, domains, software, and keys; renew before expiration; support agency certificate pinning and HSTS as applicable.

PWS 5.13.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 71-72

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.7 Annual Forms Changes (PWS 5.13.7)

STATEMENT OF WORK (PWS 5.13.7):

5.13.7 Annual Forms Changes

PWS 5.13.7, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 72

ANNUAL ROLLOVER IS GRADED AGAINST A FIXED CALENDAR DATE.

Evaluation Factor I states that the Government will consider the Vendor's "approach to annual system changes, forms rollover, data migration, and Contact Center operations, including the ability to deliver January 1 rollover releases, maintain required technical artifacts, support Systems Acceptance Testing, manage ad hoc legislative changes, preserve legacy data integrity and continuity back to 2009."

PWS 1.6.4 requires EFAST2 functions and releases to be supported and tested on New Year's Day. Address the 1 January release date and the November Systems Acceptance Test explicitly.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.7.1 Annual Forms, Schedules, and Instructions Development (PWS 5.13.7.1)

STATEMENT OF WORK (PWS 5.13.7.1):

5.13.7.1 Annual Forms, Schedules, and Instructions Development

In accordance with the dates noted on the Government-provided annual forms/instructions development schedule, the Contractor must receive a list of changes to the forms, schedules, and/or instructions. The form instructions constitute requirements for the EFAST2 system. The Contractor must create forms/instructions/rollover schedule, mock-ups of the forms, forms/schedules, and instructions containing baseline changes to dates in accordance with the Government-furnished development schedule and multiple agency-consolidated change lists. Both the development schedule and change lists are subject to change. Development of the forms, schedules and instructions must include, but is not limited to:

- The Contractor creating, revising, and assuring the quality of multiple versions of the Form 5500 Series forms, schedules, and instructions for the development of a given form year cycle.

Volume I - Technical Approach

- The Contractor's compliance with any requisite ad-hoc tasks such as minor typographical or formatting changes and/or last-minute legislative mandates requested beyond the development schedule. The Contractor must provide a full set of the updated documents in a final/clean format, as well as a full set in a marked up/red-line format that clearly exhibits the changes made to the forms, schedules, and instructions from the previous form year to the current form year. The marked up/red-line versions must only display changes made to the documents from the previous form year version. The mark-ups must not display changes made to changes throughout the development cycle or formatting changes.

The software used by the Contractor to create the mock-ups must provide resulting files that are portable to and easily editable by the Government. Additionally, the Contractor-developed forms, schedules and instructions must precisely match the existing forms, schedules and instructions in substance and in on-screen and printed form display as currently published by the Government, unless the government agrees to a change in display.

At the end of the forms development cycle, the contractor must deliver (1) PDF files and (2) source files developed using the Contractor's forms design package. The PDF files must be fillable with objects configured that map each individual field to the XML Element Name specified in that plan year's DER. Repeating elements must include a suffix number following the XML Element Name so they can be uniquely identified (i.e., ein_1, ein_2, etc.). Where duplicate names are in different sections, the Contractor must include a prefix identifying the appropriate section prior to the XML Element Name (i.e., address, city, foreign, address, city, etc.).

The final files must be provided to third-party software developers.

PWS 5.13.7.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 72

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.7.2 Annual Rollover Requirement Development (PWS 5.13.7.2)

STATEMENT OF WORK (PWS 5.13.7.2):

5.13.7.2 Annual Rollover Requirement Development

Each year, changes are needed in EFAST to accommodate a new series of Form 5500 forms and improve edit tests prior to the release of the new forms to the public on January 1. Requirements development leading up to the release begin 18 months prior to the release.

The Contractor must analyze and evaluate proposed and/or final forms, instructions, and related functional changes to determine impact on the EFAST2 system and new requirements.

The Contractor must analyze why EFAST data may incorrectly fail edit tests and recommend modifications to edit tests, forms, instructions, related functions, or filer educational material.

The Contractor must translate changes suggested by itself or other stakeholders into EFAST requirements.

The Contractor must maintain a record of suggested changes in a change list. The Contractor must clarify requirements and lead requirement clarification meetings with selected Government stakeholders and/or the EFAST vendor.

The contractor's change list must identify the unique requirement number, define the current

Volume I - Technical Approach

implementation, define the requested change, document all comments from each stakeholder group, and specify DER/schema changes needed.

The Contractor must develop and deliver rollover packages that include:

- a. A detailed summary of known changes including documentation of which organization requested or objected to the change, and XPATH for new/modified edit tests. This change list must include changes suggested by the agencies to make data more accurate and reliable.
- b. An updated Interface Requirements Document (IRD) to describe the characteristics and layout of distributions from the EFAST vendor to each of the three stakeholder Government agencies.
- c. An updated edit test mask list matrix summarizing edit tests and including dates specifying when each test must be turned on/off (e.g., masked or unmasked).
- d. A crosswalk matrix specifying requirements for attachment types.
- e. A due date table specific to filings for active processing years.
- f. A spreadsheet specifying how values of blank and zero are to be interpreted.
- g. Updates to use cases or supplemental specifications where applicable.
- h. Requested changes to web service structures or entity test algorithms (if any) The

Contractor must convert the rollover package into data element requirements and specifications in various formats for different types of users and programmers (e.g., user-friendly PDF, XML, WSDL, and XSD files).

The rollover requirements provided by the Contractor are implemented into EFAST and third-party filing software products designed to prepare and transmit returns/reports to EFAST. It is therefore important that the requirements be accurate, internally consistent, and of high quality.

Even after final rollover package is delivered, the Contractor must analyze and evaluate the completeness and accuracy of EFAST rollover requirements. In the event a requirement in the final rollover package was not specified correctly, the Contractor must notify the government immediately and take corrective actions as directed.

PWS 5.13.7.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 72-74

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.7.3 Annual Rollover Updates (PWS 5.13.7.3)

STATEMENT OF WORK (PWS 5.13.7.3):

5.13.7.3 Annual Rollover Updates

The Contractor must update and adapt EFAST2 to accommodate annual rollover changes declared by the Government through issuance of GFI, including but not limited to adjustments to data element requirements, schema, business rules, edit tests, distribution, and related downstream and/or ancillary system functionality, components, and documentation. The Contractor must work in close coordination with the Government to implement all rollover updates.

Volume I - Technical Approach

The Contractor will be responsible for implementing both the required annual system maintenance changes and a typical number of non-recurring changes into all components of the production system at no additional cost to the Government, within the prescribed schedule for rollover, and with no disruption or downtime in the production system.

The Contractor must plan to release rollover annually on January 1st. Prior to rollover, the Government plans to evaluate Annual Rollover and other changes through a Systems Acceptance Test (SAT). The Government's expectation is that only one SAT will be required annually and will occur in November. The Government reserves the right to conduct additional tests/reviews if, in the Government's determination, an excessive number of errors or security vulnerabilities have been exposed that may prevent the Government from authorizing rollover operations.

Upon rollover completion, the Contractor must continue to analyze and evaluate the completeness and accuracy of EFAST rollover requirement implementation. If rollover implementation requirements, to include implemented edit tests, are deemed by the contractor or the government to need correction, the Contractor must take corrective action outside of the annual rollover schedule and make the necessary system and documentation (DER) updates. The frequency and implementation timing of these updates will be at the discrepancy of the government and may be limited to quarterly.

PWS 5.13.7.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 74

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.7.4 Annual System Maintenance Rollover Changes (PWS 5.13.7.3)

STATEMENT OF WORK (PWS 5.13.7.3):

5.13.7.3 Annual System Maintenance Rollover Changes

The Contractor must plan to release rollover annually on January 1st. Prior to rollover, the Government plans to evaluate Annual Rollover and other changes through a Systems Acceptance Test (SAT). The Government's expectation is that only one SAT will be required annually and will occur in November. The Government reserves the right to conduct additional tests/reviews if, in the Government's determination, an excessive number of errors or security vulnerabilities have been exposed that may prevent the Government from authorizing rollover operations.

PWS 5.13.7.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 74

THIS PARAGRAPH AND THE ONE ABOVE CARRY THE SAME PWS NUMBER.

The solicitation prints 5.13.7.3 twice on page 74, once for Annual Rollover Updates and once for Annual System Maintenance Rollover Changes, with one paragraph duplicated verbatim between them. Both are given headings here and both cite PWS 5.13.7.3 as the RFQ numbers them. Raise it with the Contracting Officer.

Volume I - Technical Approach

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8 System Architecture (PWS 5.13.8)**STATEMENT OF WORK (PWS 5.13.8):****5.13.8 System Architecture**

The contractor must maintain six distinct environments, Production (including PATS), Development, Test, Customer Acceptance Testing (CAT), Disaster Recovery, and Load Testing, with non-production environments closely mirroring production to ensure reliable promotion of changes. The Contractor must implement disaster recovery, redundancy, scalability, fault tolerance, and load balancing across all environments, including Contact Center platforms and supporting systems, to minimize downtime from infrastructure failures, software issues, or other disruptions. Open source and cloud-based solutions must be used where practical.

PWS 5.13.8, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 74-75

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.1 Availability (PWS 5.13.8.1)**STATEMENT OF WORK (PWS 5.13.8.1):****5.13.8.1 Availability**

The Contractor must maintain and measure service availability across all public and Government-facing EFAST2 components, taking full responsibility regardless of whether issues stem from directly or indirectly controlled services. The architecture must incorporate data mirroring, backups, disaster recovery, CDN, and load balancing with no single points of failure, ensuring high availability and fault tolerance. Maintenance must be conducted between 1AM–3AM EST Monday–Saturday and 12AM–4AM EST Sunday; any out-of-window maintenance requires 24-hour advance Government approval and counts against availability performance standards. The system must meet a maximum RTO of 5 days and RPO of 24 hours. For factors beyond the Contractor's control, unplanned interruptions are permitted up to 24 cumulative hours per month, after which filing acceptance must resume; filers affected by interruptions or data loss within a five-minute outage window must be identified and notified to enable resubmission. All external integrations including the Contact Center, email services, and validation services must maintain uninterrupted communication with EFAST2, and any disruptions affecting end users, filing processing, or reporting count against availability standards. The Contractor must deploy system changes during non-peak periods, maintain a Government-approved Communication Plan for notifying stakeholders of planned or unplanned disruptions, and conduct root cause analysis for all unplanned production outages.

PWS 5.13.8.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 75

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.2 Scaling (PWS 5.13.8.2)

STATEMENT OF WORK (PWS 5.13.8.2):

5.13.8.2 Scaling

The Contractor must maintain a cloud-based architecture capable of automated horizontal and vertical scaling in response to performance demands, load fluctuations, functionality changes, or other planned and unplanned needs with minimal to no service interruption. Dynamic and elastic scaling technologies must be employed to both expand and contract system capacity as needed, optimizing cost and performance while ensuring all scaling actions occur within timeframes sufficient to meet performance standards. Where manual intervention is required for certain components, response times must still satisfy those standards.

PWS 5.13.8.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 75

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.3 Disaster Recovery (PWS 5.13.8.3)

STATEMENT OF WORK (PWS 5.13.8.3):

5.13.8.3 Disaster Recovery

The Contractor must ensure a geographically separate cloud-based disaster recovery site that mirrors EFAST system and production data with replication intervals meeting the required RPO and no less than every 24 hours for output records. The DR site must meet all EFAST2 performance requirements and support both failover and failback capabilities, which must be regularly tested. Following any failover event, a functioning secondary site must be restored within 30 days, ensuring no gap greater than 30 days exists without an available DR site. All replication and mirroring activities must be continuously monitored with automated alerting upon failure.

PWS 5.13.8.3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 75

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.4 Backups (PWS 5.13.8.4)

STATEMENT OF WORK (PWS 5.13.8.4):

5.13.8.4 Backups

The Contractor must ensure perform daily backups of all server operating systems and data, including EFAST2 databases, storing all backups in near-line or off-line storage separate from primary storage and retaining them for a minimum of one year. Backup and restore procedures must be Government-approved, documented as standard operating procedures, and supported by automated verification. Monthly restore tests of random sample files and at least one annual full system restore test must be conducted to validate media integrity and procedure accuracy, with results reported in the Information System Contingency Plan. All backup activities

must be continuously monitored with automated alerting, logging, and reporting, with performance and capacity analysis included in the monthly System Performance Report.

PWS 5.13.8.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 75-76

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.5 Service Level Agreement (PWS 5.13.8.5)

STATEMENT OF WORK (PWS 5.13.8.5):

5.13.8.5 Service Level Agreement

The Contractor must develop and maintain a Government-approved Service Level Agreement (SLA) tied to PWS performance standards, covering availability, incident and event response, backup and recovery, and disaster response. The SLA must define what is being promised, how delivery will be achieved and measured, consequences for non-delivery, and how the SLA will evolve over the contract lifecycle emphasizing realistic commitments, consistent performance, and swift issue resolution. Upon Government request, the Contractor must provide copies of all supporting SLAs and related contractual agreements used to maintain EFAST2.

PWS 5.13.8.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 76

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.6 Detailed System Design (PWS 5.13.8.6)

STATEMENT OF WORK (PWS 5.13.8.6):

5.13.8.6 Detailed System Design

Volume I - Technical Approach

The Contractor must maintain a Detailed System Design (DSD) documenting the complete technical architecture and satisfying all PWS functional requirements. At a minimum, the DSD must include: system design concept and architecture; functional descriptions of all hardware, software, interfaces, and database components across all environments including server names, functions, and software versions; modular relationships and end-to-end process flow diagrams; detailed data usage with capacity and scaling comparisons between test and production systems; all user interfaces and input/approval descriptions; assessment of design constraints and compatibility among proprietary, custom, and commercial components; system flexibility assessment for accommodating form and system changes; network and logical data flow diagrams showing all environment connections, network segments, servers with IP addresses and roles, and data origins, destinations, and storage locations; a data management plan covering legacy migration methodology, data mapping, security, privacy, risks, schedule, and maintenance; and cloud interoperability and portability requirements ensuring EFAST2 can fully operate across alternate cloud environments including Amazon, Azure, or equivalent and support migration to a different integrator or service provider.

PWS 5.13.8.6, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 76

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.7 System Sizing Analysis (PWS 5.13.8.7)**STATEMENT OF WORK (PWS 5.13.8.7):****5.13.8.7 System Sizing Analysis**

The Contractor must maintain a System Sizing Analysis that evaluates current and historical volumes and capacities across all system components including total, maximum, peak, and concurrent volumes measured in filings, transactions, requests, submissions, and users. Trend analysis must be used to determine scaling needs, system configuration, and staffing requirements for each component and subsystem, with deviations between past and new volume estimates highlighted and investigated.

PWS 5.13.8.7, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 76

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.8 Benchmark Report (PWS 5.13.8.8)**STATEMENT OF WORK (PWS 5.13.8.8):****5.13.8.8 Benchmark Report**

The Contractor must implement and maintain benchmark testing sufficient to demonstrate production

readiness, scalability, and system breaking points across all EFAST2 functional areas, simulating at minimum twice the estimated actual filing volume and web traffic. The Contractor must deliver an annual Benchmark Report based on measurements taken at least weekly documenting core performance metrics including database transactions per second, data transfer rates, network speeds, component processing rates, and input/output timings for all functional units and individual servers, as well as maximum capacity metrics identifying system breaking points and bottlenecks. The report must also include backup and restore benchmarks covering three restoration scenarios: single file or data element, full database collection, and complete system or server restoration. A detailed diagram and description of EFAST2's logical architecture, validation mechanisms, and logging methods must be included as part of the report.

PWS 5.13.8.8, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 76-77

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.9 System Performance Report (PWS 5.13.8.9)

STATEMENT OF WORK (PWS 5.13.8.9):

5.13.8.9 System Performance Report

The Contractor must continuously monitor all system services network, devices, circuits, and servers measuring performance against defined metrics and target expectations, with any anomalies thoroughly analyzed for root cause, applied fixes, and future implications, escalating to the COR where required. The monthly System Performance Report must include at a minimum: system failures and unscheduled downtime descriptions; uptime and downtime hours; EFAST2 website link status; backup job completion and verification dates; system capacity, current load, and horizontal and vertical scaling needs; network latency and response times; and daily, weekly, and monthly transaction metrics including database transaction rates, functional unit processing and transfer rates, concurrent users, average and peak submissions, web page hits, service requests, peak rates, CPU loads, and disk utilization. Raw monitoring data must be made available to the Government in real time, including access to system monitoring tools, month-to-date hosting expenses, and utilization quantities. The report must also document scaling and architecture usage metrics for all components, including quantities of cloud and third-party metered services consumed during the reporting period, reported in service-relevant units such as virtual server hours, server types, gigabytes stored, or transactions processed reflecting expected month-to-month variability as the system scales to meet demand.

PWS 5.13.8.9, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 77

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.10 Asset and Supplier Inventory (PWS 5.13.8.10)

STATEMENT OF WORK (PWS 5.13.8.10):

5.13.8.10 Asset and Supplier Inventory

The Contractor must maintain and regularly update a comprehensive inventory of all EFAST2 infrastructure assets and suppliers in a Government-approved format, including functional descriptions of all system and subsystem components.

PWS 5.13.8.10, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 77

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.13.8.11 Data Archival Support (PWS 5.13.8.11)

STATEMENT OF WORK (PWS 5.13.8.11):

5.13.8.11 Data Archival Support

Contractor must support DOL in its communication and coordination regarding EFAST data archival requirements, and in determining compliance with pertinent federal laws relating to the archival and destruction of Form 5500 records. This must include and is not limited to preparing and delivering annual EFAST archive files to National Archives and Records Administration (NARA) as per the existing policies and NARA requirements.

PWS 5.13.8.11, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 77

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

2.14 Transition-Out (PWS 5.14)

STATEMENT OF WORK (PWS 5.14):

5.14 Transition-Out

The contractor must provide services for Transition-Out to allow the incoming contractor to staff up to the appropriate support levels and participate in knowledge sharing with the outgoing contractor so that incoming staff can be prepared to fully support the system. During this time, the outgoing Contractor must provide support services to the orderly transition of functions from this effort to the DOL and/or successor contractor.

The contractor must be the lead on the transition activities during the transition period, leading Technical Exchange Meetings (TEMs) with the incoming contractor to impart knowledge of the system(s) developed

Volume I - Technical Approach

and activities performed under this effort, to include maintenance activities that are in progress. The TEMs must

include a demo of all components, the technology used, and a walkthrough of all documentation, to include the requirements backlog and the list of defects. The outgoing contractor must allow for the incoming contractor to 'shadow' them in obtaining knowledge of other aspects of contractual obligations other than what is discussed during the TEMs. During this period, there must be no degradation in support to the Government. At the designated turnover date (within the 30-day transition period), the successor contractor must assume full responsibility of the contract, while the outgoing Contractor focuses on contract closeout activities to complete the transition.

As part of the closeout activities, the contractor must confirm (in writing) that:

1. DOL has received draft/in-progress and final versions of all documentation (e.g., CONOPS, SOPs, requirements specifications, design specifications, configuration management plan, etc.), to include the native format of diagrams (e.g., Visio), even those embedded in documents, have been uploaded into the DOL's SharePoint project repository.
2. DOL has received all GFE and GFI, e.g., PIV badges and laptops.
3. DOL has received all source code, configurations, and database scripts.

The incumbent contractor must present its plan for transitioning the services to the successor contractor to ensure continuity of services, minimize any decreases in productivity, and prevent negative impacts on additional services during the phase out period. This initiative will contain all items listed above as well as at minimum include:

- a. Points of Contact
- b. Coordination with Government and Contractor representatives to ensure a seamless transition
- c. Status of ongoing activities
- d. Schedules and milestones
- e. Actions required of DOL
- f. Orientation and documentation to explain the tools, methodologies, and processes used in this task order
- g. Transfer of technical and project management documentation including all system/tool documentation, code, and instructions required to operate, maintain and administer systems and tools
 - o Transfer of data, license, support contracts and security codes; passwords, encryption keys, etc.
 - o Disposition of tool (s), services, and equipment used to support or test the provided services.
 - o Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI) and GFE inventory management.

PWS 5.14, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 77-79

TRANSITION-OUT IS A VOLUME II ITEM - WRITE A SHORT CONFIRMATION HERE ONLY.

PWS 5.14 is quoted above because Instructions, Volume I names "Part 5-Specific Tasks" as source material for this volume. But Transition-Out is graded under Factor II, not Factor I: the Evaluation section places "Start-Up, Transition-In, and Transition-Out approaches" and "structured knowledge transfer at contract end" under FACTOR II - MANAGEMENT APPROACH. Instructions, Volume I never mentions

Volume I - Technical Approach

Transition-Out and Factor I does not grade it.

WRITE HERE: two or three sentences confirming understanding of the PWS 5.14 obligations quoted above, and stating that the Transition-Out approach, including the closeout confirmations and knowledge transfer to a successor contractor, is provided in Volume II - Management Approach.

Instructions F: do not split the Transition-Out approach across both volumes.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3 FUNCTIONAL, SECURITY, AND COMPLIANCE REQUIREMENTS (INST. VOL I)

INSTRUCTIONS (Instructions to Vendors, Volume I):

The Vendor must submit a quotation that demonstrates a clear understanding of the RFQ, PWS, and the EFAST2 Rebuild/Modernization objectives, scope, and key requirements. The response must describe the Vendor's technical approach, methods, development practices, and tools for performing the work across the multi-platform enterprise environment, including design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration.

The Vendor must address functional, security, and compliance requirements; identify key risks and credible mitigation strategies; and demonstrate relevant experience of similar nature, scope, complexity, and risk. The response must also describe the Vendor's familiarity with large-scale federal IT modernization efforts and its approach to assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition. General or vague statements without supporting rationale or examples will not be sufficient.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 155-156

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The evaluation will consider the clarity, completeness, feasibility, and credibility of the proposed technical approach, including the Vendor's understanding of the scope of work, required technologies, methodologies, standards, and ability to manage performance risk. **The Government will assess how the proposed solution addresses functional, security, and compliance requirements, including FedRAMP, FISMA, NIST SP 800-53 Rev. 5, IRS Publication 1075, identity management and authentication, and Section 508 and WCAG 2.1 A/AA accessibility.** The evaluation will also consider the Vendor's use of AI, automation, DevSecOps, agile practices, and innovative solutions to support development, modernization, operations, and enhancement activities; reduce delivery time; maintain secure and current software; minimize vulnerabilities; and ensure continued compliance with Federal requirements.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 160

STATEMENT OF WORK (PWS 1.6.8):

1.6.8 Security Requirements: Cybersecurity requirements are specified in Technical Exhibit 3. The contractor must maintain the confidentiality, integrity, and availability of EFAST2 at the Moderate Baseline Security Category level of compliance.

PWS 1.6.8, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 18

WHY THIS IS A SECTION AND HOW ITS SUBHEADINGS WERE CHOSEN.

The phrase "functional, security, and compliance" appears nowhere in PWS Part 5. It is a cross-cutting

Volume I - Technical Approach

requirement stated directly by Instructions, Volume I and Evaluation Factor I, so there is no PWS paragraph to sequence it by and it stands as its own section.

Evaluation Factor I names six compliance regimes by name. Each has its own subheading below, in the order Factor I lists them, so an evaluator can find each one. The remaining subheadings carry the compliance requirements that have no home in Section 2: PWS 1.6.8.1, PWS 1.6.8.2, PWS 6.1 Applicable Publications and PWS 4.2 Clearance.

The functional requirements themselves are the PWS Part 5 tasks answered in Section 2. Cross-reference them here rather than repeating them.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.1 FedRAMP (PWS 1.4)

STATEMENT OF WORK (PWS 1.4):

1.4 Scope

This outlines the specific areas of work, boundaries, and services covered. ***The solution must be delivered as a cloud-based service in a Government approved and FedRAMP Authorized (Moderate) environment.***

This work involves (1) data collection, processing, and dissemination of Government forms data, (2) support of stakeholders (filers, third-party software, and Government), and (3) management services.

The scope of this work is for the Contractor to deliver the EFAST2 system while meeting the preceding objectives. The scope of the work includes the following:

- Annual Rollover Baseline Changes to operate the system for each processing year and to “rollover” in preparation for succeeding processing year
- Advanced Search & bulk download (API) features on filings
- Contact Center Operations to respond to calls, emails and web inquiries. Includes Chatbot support and user satisfaction analysis (postproduction deployment)
- Program ISO and Support to maintain designated level of system security compliance
- Program Management to maintain a stable management presence for all contractor work activities
- Quality Assurance to establish and maintain a software quality program through all phases of the system development life cycle
- Quality Control to provide an independent quality control unit to measure and report on all performance standards defined in the contract
- Software and License Agreements necessary to support the EFAST2 solution
- Internet Filing Acceptance Service (IFAS) to operate and maintain a high-performance, high-availability, and fully automated service for use by Third Party software
- Performance Monitoring of all system components
- Web Content Management to support a workflow for approved content changes
- Change Management using DevSecOps methodologies
- Third Party Developer Conference to plan and communicate EFAST2 changes (postproduction

deployment)

- Non-recurring Rollover Changes to support legislative changes (postproduction deployment) The detailed requirements of developed filing system may be refined adaptively over the course of the effort to continuously meet specified user needs. User needs will be prioritized based on business value and technical dependencies.

PWS 1.4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 14-15

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.2 FISMA and NIST SP 800-53 Rev. 5 (TE 3)

STATEMENT OF WORK (Technical Exhibit 3):

Technical Exhibit 3 Cybersecurity Clauses As determined applicable by the Government, the Contractor agrees to comply with the following statutes, regulations, standards, and policies:

- Federal Information Security Modernization Act (FISMA) of 2014
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and contractors
- The Computer Security Act of 1987
- Office of Management and Budget (OMB) Circular A-130
- Federal Information Processing Standard (FIPS) 140
- Federal Information Processing Standard (FIPS) 199
- Federal Information Processing Standard (FIPS) 200
- National Institute of Standards and Technology (NIST) Special Publication 800-53
- National Institute of Standards and Technology (NIST) Special Publication 800-160
- National Institute of Standards and Technology (NIST) Special Publication 800-161
- National Institute of Standards and Technology (NIST) Special Publication 800-171
- Trusted Internet Connections (TIC) initiative (Update), (M-19-26), September 12, 2019
- The Privacy Act
- OMB M-23-13 No TikTok on Government Devices Implementation Guidance

Note: Depending on the types and extent of access to data and systems required for the work, contractor personnel may be required to undergo a background investigation and obtain a security clearance. The contractor ensures all requirements and submissions are completed within the timeframe requested by the government. DOL reserves the right to review and approve or disapprove all the security safeguards instituted to comply with the requirements of this contract. If the Contractor fails to comply with the cybersecurity and privacy requirements, the Contractor may be deemed to have failed to perform the requirements of this contract. Contractor must include the Government's cybersecurity and privacy requirements contained in its contract in every solicitation and every subcontract associated with the work

Volume I - Technical Approach

performed under this contract. Requirements for acquiring information technology Applications provided by the contractor for use by the government must be fully functional and operate correctly as intended on systems using the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at National Checklist Program (NCP). Applications designed for normal end users must run in the standard user context without elevated system administration privileges.

No hardware, software, or service provided by the contractor may use or incorporate any hardware, software, or services developed or provided by Kaspersky Lab. No hardware, software, or service provided by the contractor may use or incorporate any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Requirements for work with Privacy Act Systems

Privacy Act notification: If applicable, the Contractor will be required to design, develop, or operate system(s) of records on individuals, to accomplish an Agency function subject to the Privacy Act of 1974, Public Law 93 579 (5 U.S.C., Section 552a) as amended (the Act), and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. The title(s) of the system(s) of records must be listed on the respective task orders, as appropriate.

The Contractor agrees to:

a. Comply with the Act and the Agency rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

o the system(s) of records; and

o the design, development, or operation work that the Contractor is to perform.

b. Include the Privacy Act provisions contained in this contract in every solicitation and every subcontract, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act.

c. Include, in all data solicitations requesting information to be placed in a Privacy Act System of Records, a Privacy Act notification statement provided by the DOL.

For Supply Chain Risk Management for contracts involving information and communications technology (ICT)

The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with Federal Acquisitions Regulation, Public Law 115-232 § 889. At minimum, the Contractor must:

TE 3, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 117-118

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.3 IRS Publication 1075 (PWS 6.1.2)

STATEMENT OF WORK (PWS 6.1.2):

IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies (dated November 2021) <https://www.irs.gov/pub/irs-pdf/p1075.pdf> IRS Encryption Requirements of

Publication 1075 (dated April 2023) <https://www.irs.gov/privacy-disclosure/encryption-requirements-of-publication-1075>

PWS 6.1.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 80

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.4 Identity Management and Authentication (PWS 5.4.2.2)

STATEMENT OF WORK (PWS 5.4.2.2):

5.4.2.2 Filer Authentication

The Contractor must implement a routine for filers to authenticate to electronically sign filings and authenticate to the EFAST2 website. Note that there can be one or more signatures provided on a single filing.

Identity Assurance Level (IAL-1) must be used for enrollment and identity proofing of the web portal authentication and electronic signatures. Authentication Assurance Level (AAL) 2 must be used for filer authentication of the web portal authentication. Identity Assurance Levels are defined by NIST SP 800-63 series.

To achieve AAL2, NIST SP 800-63 requires the enforcement of Multi-factor Authentication (MFA). The Contractor must integrate Login.gov as a secure sign-in service, at IAL-1 with multi-factor authentication into the EFAST2 web portal. All web portal users must be required to use Login.gov integrated authentication to access the EFAST2 web portal in a phased approach subject to Government approval. Filer authentication should include an attribute indicating if the authorized individual is a current Government employee (EBSA, IRS, OCA, PBGC, COR or COR representative).

EFAST2 must obtain and authenticate filer identity to the extent feasible and practical using Government-approved methods. The contractor must maintain user stories or use cases or similar documentation illustrating the filer authentication routine, including filer identity information collected/stored/passed. Any filer authentication credentials issued/stored by the contractor must be encrypted while in transit and at rest.

A filing credential may be deemed compromised if an unauthorized individual has obtained it. If this is reported, the contractor must revoke the credential. No filing will be accepted using a revoked credential. In

the event of revoked credentials, the Contractor must offer to transfer previous filings to a new account should the user need to retain access to their previous filing information in accordance with Government-approved procedures.

Filer accounts may only be locked/revoked by the Contractor based on valid user requests.

PWS 5.4.2.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 46-47

THE DETAILED RESPONSE BELONGS IN SECTION 2.

Volume I - Technical Approach

Identity management and authentication is performed work, and the PWS puts it in Part 5: PWS 5.4.1 Registration Portal and PWS 5.4.2.2 Filer Authentication, both answered at Section 2. PWS 1.3 objective 1 requires registration and credentialing "aligned to NIST SP 800-63 digital identity guidelines (e.g., IAL-1, AAL2 for authentication), and integrate with Government-approved identity providers via standards (SAML 2.0 or OIDC/OAuth 2.0)."

Write a short compliance summary here and cross-reference Section 2. Do not duplicate the technical approach.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.5 Section 508 and WCAG 2.1 A/AA Accessibility (TE 4)**STATEMENT OF WORK (Technical Exhibit 4):*****Technical Exhibit 4 Section 508 Compliance Clauses*** Section 508 Background

Electronic and Information Technology (EIT)/Information and Communication Technology (ICT) greatly affects how federal agencies, and their employees achieve agency goals, do their daily work and serve the American people. EIT/ICT is also a major gateway to employment opportunities in both the public and private sectors, and it is key to how information is shared with employees, how employees are productive in the workplace, and how they advance in their careers. General Requirements

All EIT/ICT deliverables produced by the CONTRACTOR must be accessible, usable by assistive technologies, and meet the baseline criteria outlined in Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) August 7, 1998, the Web Content Accessibility Guidelines 2.0 (WCAG 2.1 A and AA) and the Department of Labor Management Series (DLMS) Section 9, Chapter 600. EIT/ICT deliverables include but are not limited to websites, software, mobile applications, webcasts, webinars, multimedia (e.g., charts, graphs, graphics, videos, audio tracks, and animation), social media, collaborative workspaces and tools, documents (e.g., PDF, PowerPoint, Excel, and Word), forms and field elements, data tables, image maps, and any training and related training materials. Print materials must be made available in an alternate accessible format when requested. By submitting deliverables pursuant to this contract, CONTRACTOR is certifying that such deliverables are conformant with the accessibility guidelines referenced above.

Acceptance and Conformance

By submitting deliverables pursuant to this contract, Contractor is certifying that such deliverables are conformant with the accessibility guidelines referenced above. The Contractor must include certification of conformance to accessibility standards with all deliverables, and such certification must be in the form and format defined by the COR. Proof of adequate accessibility, including design, development, and testing data must be provided to the COR upon request.

Acceptance of deliverables by the Government does not constitute agreement that the deliverables are conformant, and the Government reserves the right to evaluate such deliverables within a reasonable time to assess the Contractor's certification of accessibility and conformance. Government evaluations, when conducted, will utilize unified test approaches, when applicable, or other appropriate testing methodologies approved by the DOL Section 508 Program Office. Deliverables that are found to be non-conformant will be remediated by the Contractor within a reasonable time and at no additional cost to the Government.

TE 4, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 123-124

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.6 Physical Security (PWS 1.6.8.1)

STATEMENT OF WORK (PWS 1.6.8.1):

1.6.8.1 Physical Security

The contractor must be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials must be secured.

PWS 1.6.8.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 18

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.7 Conservation of Utilities (PWS 1.6.8.2)

STATEMENT OF WORK (PWS 1.6.8.2):

1.6.8.2 Conservation of Utilities

The contractor must instruct employees in utilities conservation practices. The contractor must be responsible for operating under conditions that preclude the waste of utilities.

PWS 1.6.8.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 18-19

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.8 Applicable Publications (PWS 6.1)

STATEMENT OF WORK (PWS 6.1):

6.1 Publications Applicable to This PWS:

From time-to-time Government standards will change and new related standards will be introduced. The

Volume I - Technical Approach

Contractor must ensure that it complies with the most current version of Government standards cited herein as well as changes to those standards and new related standards. If there are changes that significantly impact operations, the Government will work collaboratively with the Contractor to determine an expeditious approach for working through the technical, contractual, and/or cost implications, and implement the changes within a prescribed schedule.

The publications must be coded as mandatory or advisory and the date of the publication are applicable to the requirement. All publications listed are available via the Internet.

PWS 6.1, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 79

STATEMENT OF WORK (PWS 6.1.5):**6.1.5 Section 508 Compliance**

In order to meet Section 508 accessibility requirements for all Information and Communication Technology (ICT) procured, maintained, developed or used by the Contractor at, or on behalf of, DOL – to include electronic documents, software, websites and webpages created or maintained by the Contractor and the deliverables listed above – the Contractor must:

1. Provide summary narrative text descriptions or a data table describing each complex graphic (e.g., pie graphs, line graphs, maps, bar graphs, flow charts) in a separate comma-separated values/character-separated values (CSV) file.
2. Label each figure or graphic image with an alternate text description. ***Ensure Contractor support staff producing ICT deliverables have a solid working knowledge of Section 508 and can perform Quality Assurance Testing for Section 508 and the applicable WCAG 2.1 A and AA success criteria.*** Verification of such knowledge must be provided for the individuals proposed on the contract.
3. Have updated authoring and testing tools to produce Section 508 output on their own (The Government will not provide these tools.).
4. Provide two digital copies of any report over 25 pages in media formats readable by Windows-based programs; one copy formatted in Microsoft Word and the second in the Portable Document Format (PDF). Color and/or black & white PDFs are acceptable.
5. Reports must not be submitted in HTML format, unless specifically requested by the specifications. The Section 508 Standards described herein provide the minimum Government requirements and do not, in any way, diminish the Contractor's responsibility to meet additional requirements that may be applicable under the law.

PWS 6.1.5, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 81

PWS 6.1.5 CONTAINS A PERSONNEL-VERIFICATION SENTENCE THAT MAY BE A SUBMISSION REQUIREMENT.

PWS 6.1.5 states: "Verification of such knowledge must be provided for the individuals proposed the contract." Read literally that asks for evidence of Section 508 and WCAG 2.1 A/AA competence for proposed individuals.

Nothing in the Instructions to Vendors asks for it, and PWS 1.6.10 makes resumes a post-award

Volume I - Technical Approach

submission. The sentence is also grammatically incomplete. Ask the Contracting Officer whether any verification is due with the quotation. Until answered, state the approach in the narrative rather than attaching personnel evidence.

Related: PWS 1.6.10 requires the Test Engineer to hold DHS Trusted Tester certification or to be able to gain it within 90 days.

PWS 6.1.1 Laws and PWS 6.1.2 Federal Guidance are marked Mandatory. PWS 6.1.3 Industry standards and PWS 6.1.4 DOL specific standards are marked Advisory. PWS 6.1.4 states the DOL-specific standards "are available upon award," so they cannot be reviewed before submission.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

3.9 Clearance (PWS 4.2)

STATEMENT OF WORK (PWS 4.2):**4.2 Clearance**

The contractor must possess or be eligible to receive and maintain a National Agency Check with Inquiries (NACI) clearance. The contractor's employees, performing work in support of this contract action must have been granted a NACI security clearance and must receive clearance to onboard from DOL prior to commencing work.

PWS 4.2, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Page 39

CLEARANCE IS A PERFORMANCE PREREQUISITE, NOT A SUBMISSION ITEM.

PWS 4.2 requires NACI clearance and DOL onboarding approval before work begins, and Technical Exhibit 2 deliverable TE2#1 makes personnel suitability packages due 14 calendar days from award. Nothing in the Instructions to Vendors requires clearance evidence with the quotation. Describe the approach; do not attach clearance documents.

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

4 KEY RISKS AND CREDIBLE MITIGATION STRATEGIES (INST. VOL I)

INSTRUCTIONS (Instructions to Vendors, Volume I):

The Vendor must submit a quotation that demonstrates a clear understanding of the RFQ, PWS, and the EFAST2 Rebuild/Modernization objectives, scope, and key requirements. The response must describe the

Vendor’s technical approach, methods, development practices, and tools for performing the work across the multi-platform enterprise environment, including design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration. The Vendor must address functional, security, and compliance requirements; **identify key risks and credible mitigation strategies**; and demonstrate relevant experience of similar nature, scope, complexity, and risk. The response must also describe the Vendor’s familiarity with large-scale federal IT modernization efforts and its approach to assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition. General or vague statements without supporting rationale or examples will not be sufficient.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 155-156

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

Key Risk	Credible Mitigation Strategy	PWS or Technical Exhibit Reference
[Insert risk]	[Insert mitigation]	[Insert reference]
[Insert risk]	[Insert mitigation]	[Insert reference]
[Insert risk]	[Insert mitigation]	[Insert reference]
[Insert risk]	[Insert mitigation]	[Insert reference]
[Insert risk]	[Insert mitigation]	[Insert reference]

Exhibit 1-6. Key Risks and Mitigation Strategies (Inst. Vol I)

5 RELEVANT EXPERIENCE AND FAMILIARITY WITH LARGE-SCALE FEDERAL IT MODERNIZATION (INST. VOL I)

INSTRUCTIONS (Instructions to Vendors, Volume I):

The Vendor must submit a quotation that demonstrates a clear understanding of the RFQ, PWS, and the EFAST2 Rebuild/Modernization objectives, scope, and key requirements. The response must describe the Vendor's technical approach, methods, development practices, and tools for performing the work across the multi-platform enterprise environment, including design, development, architecture, DevSecOps, AI and innovative solutions, security and compliance, operations and maintenance, contact center support, filing acceptance services, third-party integration, annual rollover, data dissemination, and data migration. The Vendor must address functional, security, and compliance requirements; identify key risks and credible mitigation strategies; and **demonstrate relevant experience of similar nature, scope, complexity, and risk. The response must also describe the Vendor's familiarity with large-scale federal IT modernization efforts** and its approach to assuming full contractual responsibility within thirty (30) days of award while minimizing the need for Government resources during transition. General or vague statements without supporting rationale or examples will not be sufficient.

Instructions Vol I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 155-156

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, electronic filing or data collection systems, cloud-based federal environments, third-party software support and certification programs, contact center operations, and agile software development. The Government will assess whether the Vendor's experience, lessons learned, and technical approach reduce performance risk and support successful performance, including the ability to assume full contractual responsibility within thirty (30) days of award with minimal Government involvement in knowledge transition. The evaluation will also consider the Vendor's approach to annual system changes, forms rollover, data migration, and Contact Center operations, including the ability to deliver January 1 rollover releases, maintain required technical artifacts, support Systems Acceptance Testing, manage ad hoc legislative changes, preserve legacy data integrity and continuity back to 2009, meet Technical Exhibit 1 performance standards, and use AI-enabled capabilities for self-service support, PII detection and redaction, and analysis of unstructured documents. The Government is approach-neutral and will assess the extent to which the proposed solution best meets the stated requirements, schedule, risk profile, and total cost of ownership.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

Key Performance Area Named in Factor I	Contract or Program	Nature, Scope, Complexity and Risk	Proposed Approach for This Area
Large-scale federal IT modernization	[Insert]	[Insert]	[Insert]
Electronic filing or data collection systems	[Insert]	[Insert]	[Insert]
Cloud-based federal environments	[Insert]	[Insert]	[Insert]
Third-party software support and certification programs	[Insert]	[Insert]	[Insert]
Contact center operations	[Insert]	[Insert]	[Insert]
Agile software development	[Insert]	[Insert]	[Insert]

Exhibit 1-7. Relevant Experience by Factor I Key Performance Area (Evaluation Factor I)

5.1 Large-Scale Federal IT Modernization (Evaluation Factor I)

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including **large-scale federal IT modernization**, electronic filing or data collection systems, cloud-based federal environments, third-party software support and certification programs, contact center operations, and agile software development.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

5.2 Electronic Filing or Data Collection Systems (Evaluation Factor I)

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, **electronic filing or data collection systems**, cloud-based federal environments, third-party software support and certification programs, contact center operations, and agile software development.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Volume I - Technical Approach

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

5.3 Cloud-Based Federal Environments (Evaluation Factor I)**EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):**

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, electronic filing or data collection systems, **cloud-based federal environments**, third-party software support and certification programs, contact center operations, and agile software development.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

5.4 Third-Party Software Support and Certification Programs (Evaluation Factor I)**EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):**

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, electronic filing or data collection systems, cloud-based federal environments, **third-party software support and certification programs**, contact center operations, and agile software development.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

5.5 Contact Center Operations (Evaluation Factor I)**EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):**

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, electronic filing or data collection systems, cloud-based federal environments, third-party software support and certification programs, **contact center operations**, and agile software development.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.

5.6 Agile Software Development (Evaluation Factor I)

EVALUATION CRITERIA (Evaluation, Factor I - Technical Capability):

The Government will evaluate the relevance and quality of the Vendor's prior experience and proposed approach for key performance areas, including large-scale federal IT modernization, electronic filing or data collection systems, cloud-based federal environments, third-party software support and certification programs, contact center operations, and *agile software development*.

Evaluation Factor I, Attachment A19 - 1605TA-26-Q-00055, Solicitation, Pages 160-161

Start typing your response here. When done, remove all the boxes and the text that appears in the boxes above. That text is for your reference only.