U.S. Department of Transportation

# Privacy Impact Assessment

## Federal Aviation Administration (FAA)
## Office of Information & Technology Services (AIT)
## Information Technology Innovative Procurement for Strategic Sourcing (ITIPSS) Contract Administration Tool (ICAT)

### Responsible Official

Tami Branham
Email: Tami.Branham@faa.gov
Phone Number: 405-501-4396

### Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

## Executive Summary

The Federal Aviation Administration's (FAA) Office of Information & Technology Services (AIT), Innovative Procurement Strategic Sourcing (ITIPSS) Program Office (ASP-400) is developing a commercially available Contract Lifecycle Management (CLM) tool to help manage a large, multiple-award, indefinite-delivery, indefinite-quantity (IDIQ) contract. The ITIPSS Contract Administration Tool (ICAT) will aid ASP-400 in administering task orders issued against the ITIPSS contract.

This Privacy Impact Assessment (PIA) is being performed under the E-Government Act of 2002, because ICAT collects Personally Identifiable Information (PII), including resume information, on members of the public who are individuals who work for contractor companies that do business with the FAA. ICAT was developed to comply with Section 348 of Public Law 104-50 and the FAA's Acquisition Management Policy which requires contractor personnel with specific expertise, knowledge, skill, or experience to help implement or improve the FAA's systems, programs, functions, or goals.

## What is a Privacy Impact Assessment?

*The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.*[1]

*Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protecting the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:*

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

*Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.*

## Introduction & System Overview

The Office of Information & Technology Services (AIT), Innovative Procurement Strategic Sourcing (ITIPSS) Program Office (ASP-400) uses the ITIPSS Contract Administration Tool (ICAT) system to administer task orders issued against the ITIPSS contract. ICAT is FedRAMP authorized. ICAT offers the following services:

1. **Documentation Storage:** This feature securely retains all documents inputted. This includes every contract, task order, modifications, pre-award, and post-award documents, and resumes for approval based on set criteria such as meeting educational requirements. While resumes may hold potential candidates' (PII), only authorized FAA personnel and contractors can view them. The system also records contractor labor rates, deliverables per task order, proprietary data, and performance ratings.

    - **Monitoring Strategy:** Regular audits of access logs to ensure only authorized users view sensitive data (for example, PII) and automated alerts for any unauthorized access attempts.

2. **Document Generation:** Documents are produced using the FAA's version-controlled template.

    - **Monitoring Strategy:** Maintain version logs and monitor any unauthorized template changes.

3. **Document Workflows/Collaboration:** Users can customize workflows, digitally sign documents through Personal Identity Verification (PIV) card verification, and set reminders for pending reviews or approvals. Alerts notify users of major milestones.

    - **Monitoring Strategy:** Track the progression of documents through the workflow to ensure timely reviews and approvals.

4. **Task Order Administration:** The FAA can issue, adjust, and manage solicitations. This includes Q&A sections, downloading capabilities, tracking financial metrics,

deliverables, and overtime requests detailing the requestor's information and reasoning.

- **Monitoring Strategy:** Regularly review task order modifications and monitor for any discrepancies in deliverables PII collection (where applicable- see Attachment 1).

5. **Security/Integrations:** ICAT requires PIV-card authenticated accounts with multi-factor authentication and is Section 508 compliant. FAA can customize user permissions.

    - **Monitoring Strategy:** Continuously monitor for security breaches, and regularly update and test security protocols.

The majority of the data in ICAT relates to contract solicitations and deliverables and does not include PII. However, in fulfilling certain contractual requirements, the contracting company does have to provide some PII to the FAA about their employees. Therefore, in a typical transaction involving PII from members of the public, once a contract is awarded, a contractor company attends a kickoff meeting with a Contracting Officer's Representative (COR), who advises the contractor company on what documentation they are required to submit to the FAA in accordance with the performance of the contract. Each contractor company will receive an email from the COR with instructions on how to access ICAT and what documents must be submitted. All documentation that the contractor company is required to submit occurs with a template that is provided by the FAA. The purpose of this template is to limit the amount of information provided to the FAA. Each template contains language instructing the contractor company to not input unnecessary PII.

Contractor companies are required to submit resume information on individuals they expect to use to fulfill FAA contracts. The contractor company is required to use an FAA-supplied template to provide this information (under OMB approval 2120-0592, expiration date 3/31/2024). PII expected to be provided to the FAA includes name, business email address, education levels, qualifications, and previous work experience. The FAA-supplied template reminds the contractor company to not add PII such as home address. The resume is then work-flowed through ICAT with the end goal being approval by the FAA COR. Whether approved or denied, the contractor company is informed via notification within ICAT.

In addition to resume information, contractor companies provide PII in a variety of reports, such as a monthly status report, waiver requests, teleworking agreements, government-furnished equipment requests, etc. For a complete list of Reports and use of PII in ICAT, see Appendix 1.

Searches of substantive records relating to the primary purpose of the system are expected to be made with contract numbers and task numbers, and not individual PII. Audit logs are expected to be created and may include a username/FAA email address.

## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risks. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3*[2]*, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[3].

## Transparency

*Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.*

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII. All procurement activities at the FAA are performed under the FAA's Acquisition Management Policy. The FAA's Acquisition Management Policy requires all contractor companies to comply with applicable FAA privacy policy and requirements in accordance with Section 348 of Public Law 104-50.

Members of the public who work for contractor companies provide their contractor companies with resume information. The contractor company then provides that information to the FAA within ICAT, using a pre-defined template meant to limit the provision of PII. PII in ICAT is retrieved by contract number or task order number and is not retrievable by a unique identifier tied to an individual and is therefore not subject to a System of Record Notice (SORN). This template complies with the Paperwork Reduction Act and has been assigned Office of Management and Budget Control Number 2120-0595.

The publication of this PIA on the DOT Privacy website further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

## Individual Participation and Redress

*DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

ICAT is used internally by FAA employees and contractors to process contract requirements, such as work products, contract information, and resume submissions for contractor company prospective employees. Individuals are responsible for providing accurate information to their contractor companies. The contractor companies are then required to accurately provide that information to the FAA using pre-defined templates that limit the provision of PII to the FAA. Individuals who have made errors in their information must work with their contractor company to update their information in ICAT.

Searches of substantive records relating to the primary purpose of the system are expected to be made with contract numbers and task order numbers, and not individual PII, and are therefore not subject to a SORN. Therefore, members of the public should not contact the Privacy Office to request searches of their information.

## Purpose Specification

*DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.*

All procurement activities at the FAA are performed under the FAA's Acquisition Management Policy. The FAA's Acquisition Management Policy requires all contractor companies to comply with applicable FAA privacy policy and requirements in accordance with Section 348 of Public Law 104-50.

The majority of the data in ICAT relates to contract solicitations and deliverables and does not include PII. However, in fulfilling certain contractual requirements, the contracting company does have to provide some PII to the FAA about their employees, who have not yet been approved for work on the contract and are thus members of the public. Specifically, in accordance with AMS procurement guidance T3.8.2, *Support Services Contracting* requires contractor personnel with specific expertise, knowledge, skill, or experience to help implement or improve the FAA's systems, programs, functions, or goals. When support services are obtained on a time and materials or labor-hour basis, the Contracting Officer (CO) and program official/Contracting Officer's Representative (COR) should ensure the offeror proposes specific personnel for the labor categories, and provide a resume for each proposed person to determine the proposed personnel meet position requirements for CO approval. A review of the individual's resume and qualifications is used to adhere to this guidance. Attachment 1 of this PIA specifies each location where the member of the public PII is collected, and for which documented purpose.

## Data Minimization & Retention

*DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.*

The FAA collects and maintains only the minimum PII necessary for the FAA to fulfill its contractual requirements. The specifics of the collected PII are detailed in Attachment 1. ICAT also provides instructions and templates that require the contractor company to limit the PII they provide to the FAA. Additionally, ICAT chooses to minimize PII, for instance, to monitor telework, by only collecting city, state, and zip for telework location. By confining PII collection to the essentials, FAA/AIT underscores its dedication to upholding individual privacy rights and aligns with DOT's overarching aims of ensuring transparency, cultivating public trust, and adhering to federal data protection mandates.

Substantive records relating to contractual management are retained and disposed of in accordance with General Records Schedule 1.1, item 010, Financial Management and Reporting Records. Financial transaction records are destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

The system access records are retained and disposed of by the FAA in accordance with National Archives and Records Administration General Records Schedule 3.2, item 130, *Information Systems Security Records*. These records are destroyed when business use ceases. General Technology Management Records are maintained according to General Records Schedule 3.1, 020. Records maintained under item 020 are destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

## Use Limitation

*DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.*

The majority of the data in ICAT relates to contract solicitations and deliverables and does not include PII. However, in fulfilling certain contractual requirements, the contracting company does have to provide some PII to the FAA about their employees. However, PII in ICAT is not retrievable by a unique identifier tied to an individual and is therefore not subject to a System of Record Notice. The FAA does not share any PII provided by the contractor company with external entities.

Audit log information collected by the FAA to monitor and enforce access to ICAT is used only as specified by the FAA's system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records*. The information collected in these audit logs only includes information on FAA employees and not members of the public. In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use under 5 U.S.C. § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in approved investigations of improper access or usage of DOT computer systems;
- To an actual or potential party or his or her authorized representative for the purpose of negation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies where required by law.

The Department has also published 17 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019, under "Prefatory Statement of General Routine Uses."

## Data Quality and Integrity

*In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).*

The majority of the data in ICAT relates to contract solicitations and deliverables and does not include PII. However, in fulfilling certain contractual requirements, the contracting company does have to provide some PII to the FAA about their employees. This information is resume information, and it is the responsibility of the individual to provide their contracting company with current and accurate information. If updates are needed after the information has been submitted to the FAA, it is the contractor company's responsibility to coordinate any edits.

## Security

*DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure,* *as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.*

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the FISMA and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of Dec. 10, 2020).

ICAT implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege is used to grant access to FAA federal employees and contractors who require access to ICAT. In AIT's commitment to safeguarding PII, we have implemented a robust three-tiered strategy. Firstly, on an administrative level, we have instituted clear protocols and a training program to educate our staff on the importance of data privacy, ensuring they are well-versed in the stipulations of the Privacy Act. Secondly, from a technical standpoint, we employ cutting-edge encryption technologies and multi-layered cybersecurity defenses to thwart unauthorized access and maintain data integrity.

Our commitment to maintaining robust security controls is demonstrated through comprehensive documentation and annual audits conducted in accordance with iSite FedRAMP Moderate Authorization. Lastly, on the physical front, we have fortified our infrastructure with stringent access controls, surveillance mechanisms, and secure storage solutions. In the event of any privacy incidents, our immediate response is governed by well-delineated procedures in line with the OMB policies and guidance, ensuring swift, efficient, and compliant action.

## Accountability and Auditing

*DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.*

The FAA's Office of Information Security & Privacy Service (AIS) Security Governance Division is responsible for the administration of FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121A defines the various privacy requirements of the *Privacy Act of 1974*, as amended (the Privacy Act), the *E-Government Act of 2002* (Public Law 107-347), the *Federal Information Security Management Act (FISMA)*, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII.

Federal and contract employees are given clear guidance on their duties, as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. In addition, staff are required to acknowledge understanding of the FAA Privacy Rule of Behavior (ROB) and agree to them before being granted access to FAA information systems. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of ICAT relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*

To ensure adherence to all applicable privacy protection mandates, we've instituted a comprehensive framework. Governance controls have been established to clearly define roles, responsibilities, and procedures, ensuring every member of the organization is aligned with our privacy objectives. Lastly, our assessment controls involve a monitoring strategy with periodic audits and reviews, guaranteeing that our processes not only comply with existing standards but also minimize any privacy risks to individuals. ICAT performs the following auditing activities:

1. **Basic Contract Status Report (BCSR)**
   - **Strategy:** Periodically audit the stored reports to ensure only the name is collected. Regularly purge old reports after a defined retention period. Access control measures are to be set to restrict unauthorized access.
2. **Manpower Report**
   - **Strategy:** Encrypt all emails and addresses in the database. Ensure data minimization by checking that only required fields (Name, Email, Address, etc.) are filled out. Regular audits to cross-check adherence.
3. **Monthly Status Report (MSR)**
   - **Strategy:** Access control measures for report viewership. Encrypt sensitive information and ensure only names are captured. Perform routine checks to ensure compliance.
4. **Monthly Financial Report (MFR)**
   - **Strategy:** Restrict access to only financial teams and relevant stakeholders. Regularly review and purge outdated reports. Encrypt sensitive name data.
5. **Government Furnished Equipment (GFE) Report**
   - **Strategy:** Implement biometric or two-factor authentication for access. Regularly review logs to ensure only relevant personnel are accessing the reports.
6. **Other Direct Costs (ODCs) Approval Request**
   - **Strategy:** Utilize secure channels for all approval requests. Restrict and log access, ensuring that only names are collected.
7. **Travel and Training Authorization Request**
   - **Strategy:** Store requests in a secure, encrypted database. Periodic reviews to ensure only names are captured and used.
8. **Labor Category Requirement Waiver Request**
   - **Strategy:** Limit access to the HR and management teams. Encrypt education data and name in storage.

9. **Excess/Overtime Hours Request**
    - **Strategy:** Implement strict access controls and periodic audits. Ensure only names are collected and stored securely.
10. **Attachment D TORP Template, A, B.1, B.2, C, and E**
    - **Strategy:** Secure storage with encrypted fields for names. Regular purging of outdated forms. Implement two-factor authentication for access.
11. **Attachment D.1, D.2, and Appendix C**

- **Strategy:** Ensure no PII data is inadvertently added. Regular audits to ensure compliance.

12. **Log On to iSite/User accounts**

- **Strategy:** Two-factor authentication for all users. Encrypt emails and phone numbers in the system. Regularly review user logs for suspicious activities.

For all documents, the following is performed:

- Employ a dedicated data protection officer (DPO) to oversee PII protection across all deliverables and documents. The DPO will be an ASP-400 Branch Manager.
- Conduct frequent training sessions for all personnel handling these documents about the importance of PII protection and best practices.
- Set up a mechanism for real-time breach detection and immediate response.
- Regular backups of data to ensure data integrity, with a focus on encrypted backups for sensitive information.

Our risk management approach is holistic, integrating both preventative and responsive strategies to address potential threats, while regularly updating our policies to meet the evolving privacy landscape. These integrated mechanisms underscore our unwavering commitment to upholding the highest privacy standards.

## Responsible Official

Tami Branham
Email: Tami.Branham@faa.gov
Phone Number: 405-501-4396

## Approval and Signature

Karyn Gorman
Chief Privacy Officer
DOT Chief Privacy Office

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.04.01 16:24:53 -04'00'

# Attachment 1- PII in the ICAT System

| Document Name | Description | Reference: | PII Yes/No | PII Type |
|---|---|---|---|---|
| **BASIC CONTRACT DELIVERABLES (IDIQ)** | | | | |
| Basic Contract Status Report (BCSR) | The Basic Contract Status Report (BCSR) is a report to provide a high-level dashboard view of the overall basic contract performance. This report cumulates important information from each Task Order’s Monthly Status Report (described in PWS Section C.4.2.1 “Monthly Status Report (MSR)”) with a summary column for the entire program. The BCR is due no later than the 15th of each calendar month. | SIR/ITIPSS Contract C.4.1<br>PWS Section C.4.2.1 | Yes | Name and Last Name |
| Manpower Report | The Contractor must provide a monthly Manpower Report under the Basic Contract. The Manpower Report must be provided in Microsoft Excel format and easily sorted to identify manpower resources at the IDIQ-level delineated by Task Order. This report furnishes a list of detailed information for all personnel supporting all tasks. The Manpower Report is due no later than the 15th of each calendar month. | SIR/ITIPSS Contract C.4.1 | Yes | Name and Last Name, Email, Address, IF teleworking only includes: City, State, and Zip |
| **TASK ORDER DELIVERABLES** | | | | |
| Monthly Status Report (MSR) | **The Monthly Status Report (MSR)** must report the status of each Task Order awarded for the period of one month as well as cumulative view of the entire task order period of performance. The MSR will serve as the guiding management document for all contract activities and will also formally report the dollars spent on subcontracting to Small Businesses. | SIR/ITIPSS Contract C.4.2 | Yes | Name and Last Name |
| Monthly Financial Report (MFR) | The Contractor must provide a **Monthly Financial Report (MFR)** when required in a Task Order. The MFR must include the status of the current funding levels, current labor hours and dollars spent, as well as a comparison between planned and actual expenses. The MFR must be segregated by each individual Task Order. | SIR/ITIPSS Contract C.4.2 | Yes | Name and Last Name |
| Government Furnished Equipment (GFE) Report | The Contractor must report all **Government Furnished Equipment (GFE)** issued to the Contractor’s employees under each Task Order on a monthly basis. | SIR/ITIPSS Contract C.4.2 | Yes | Name and Last Name |
| Other Direct Costs (ODCs) Approval Request | **Other Direct Costs (ODCs) Approval Requests** will be required for Task Orders when the Contractor is required to purchase ODCs (reference PWS Section C.7 “Other Direct Costs”). | SIR/ITIPSS Contract C.4.2, PWS Section C.7 | Yes | Name and Last Name |
| Travel and Training Authorization Request | **Travel Authorization Requests** will be required for Task Orders when the Contractor is required to travel and/or obtain training (reference PWS Section C.6 “Travel” and PWS Section C.9 “Training”). These requests must comply with the FAA’s Contractor Training Approval Process. | SIR/ITIPSS Contract C.4.2 PWS Section C.6 & PWS Section C.9 | Yes | Name and Last Name |
| Labor Category Requirement Waiver Request | The Contractor must submit an “ITIPSS Labor Category Waiver Form” in the event that a waiver of any labor category requirement is necessary. The specific format must be approved by the Contracting Officer’s Representative and Contracting Officer. | SIR/ITIPSS Contract C.4.2 | Yes | Name and Last Name, Education |
| Excess/Overtime Hours Request | “Overtime” is defined in SIR SECTION B.4.1.6.1, Application of Overtime and H.22 Application of Overtime. As described in PWS Section C.3.3 “Hours of Work,” the Contractor must request additional hours support based on the requirements in the individual Task Orders. As necessary, the Contractor must submit an “Excess/Overtime Hours Request.” The specific format must be approved by the Contracting Officer’s Representative | SIR/ITIPSS Contract C.4.2, PWS C.3.3 | Yes | Name and Last Name |
| **SOLICITATION AND AWARD DOCUMENTS** | | | | |
| Attachment D - TORP Template (Incorporated within this document are the following templates:<br>- Attachment A- Performance Work Statement/Statement of Objectives/Stament of Work<br>- Appendix A - FAA Sensitive Data NDA<br>- QASP (Guidance for how to develop a QASP here https://fast.faa.gov/docs/CORHandbook.docx)<br>- Evaluation Factors and Methodology | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 3.1, ITIPSS Ordering Guidelines 2.1 | Yes | Name and Last Name |
| Attachment A - ITIPSS TO COR Nomination Form | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | Yes | Name and Last Name |
| Attachment B - Cost/Price Tables | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | No | |
| Attachment B.1 -Conflict of Interest (COI) template | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | Yes | Name and Last Name |
| Attachment B.2 - Non-Disclosure Agreement (NDA) template | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | Yes | Name and Last Name |
| Attachment C - Memo to Exercise TO Option | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 9.3 | Yes | Name and Last Name |
| Attachment D.1 - TORP Question and Answer | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | No | N/A |
| Attachment D.2 - TORP Question and Answer Response | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | No | N/A |
| Attachment E - Resume Template | Part of the TORP package and/or post award document | ITIPSS TORP Teamplate (list of TORP documents) | Yes | Name and Last Name, Education |
| Appendix C - Guide For Estimating Labor Costs and IGCE template | Part of the TORP package and/or post award document | ITIPSS Ordering Guidelines 2.1 | No | N/A |
| Log On to iSite/User accounts | FAA personnel, FAA CTR, Vendors (in the future), MSM Group | | Yes | Name and Last Name, Email, Possibly Phone number for Authentication |