United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Taxable Travel Relocation System (TTRS)

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: December 26, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Department of Justice (DOJ) Taxable Travel Relocation System (TTRS) is a version of the mLINQs Hosting Solution that has been configured to meet certain regulatory and policy requirements. These requirements are cited below (e.g., the applicable federal statutes, regulations, and policies -- ranging from the entitlements to the taxes assessed on the individual to the documentation required for justification and internal controls associated with payments). The mLINQs Hosting Solution is a fully functional software as a service (SaaS) system designed for government agencies to manage employee relocations and taxable travel payments.

TTRS automates the entire expense management lifecycle for processing a federal employee's relocation or travel that is taxable per IRS regulation after HR actions of identifying positions and employees who shall be relocated. Only those employees identified by the Department will be transferred or relocated. This system manages that process. For additional information of HR actions associated with requirements and processes of identifying employees who are eligible to be relocated, Department HR officials must be contacted as this system does not manage that process or regulate those decisions.

After configuration by DOJ, aligned with relocation and travel allowable entitlements as well as DOJ policy for required allowances and optional allowances based upon types of employees and location of moves, such as domestic or foreign, the system provides automated pre-move cost calculations for all relocation allowances including third party services to support accurate commitment and obligation of funds. For payments, TTRS tracks, electronically audits, and enforces system compliance through configuration and not allowing or allowing certain entitlements based upon specific types of relocations in line with travel regulations and DOJ travel and relocation policy for processing all employee vouchers and associated third party invoices. For greater payment accuracy, it tracks the issuance of advances and offsets balances due to the employee upon vouchering.

In accordance with Section 208 of the E-Government Act of 2002, the Justice Management Division (JMD) has conducted a privacy impact assessment because TTRS collects personally identifiable information (PII) from members of the public.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The entitlements for relocation are complex and compounded when taxability is applied. The information collected for TTRS is used for administrative purposes, as needed to satisfy the requirements of 26 C.F.R. § 31.3402(g)-1 and applicable state tax laws. TTRS serves to assist administrative staff in accurately and consistently calculating entitlements, taxation, and associated withholdings for employee relocation and taxable travel. The consistency in calculations provided by TTRS helps to ensure compliance with the Federal Travel Regulation and Internal Revenue Code.

To manage entitlements for relocation, the DOJ TTRS uses a Federal Risk and Authorization Management Program (FedRAMP)[1] Software as a Service (SaaS) cloud system mLINQS Hosting Service (MHS). All System Users (e.g., application users and mLINQS privileged users) access MHS over the internet. DOJ users access the MHS application via a web browser to the MHS managed website. DOJ system integrations with MHS include, but are not limited to, Unified Financial Management System for payments and DOJ Federation Services for single sign-on.

MHS operates within a shared responsibility security model that includes the following three entities: mLINQS, Azure, and the government customer(s). Each entity has the responsibility for maintaining its authorization boundary for security and compliance in practice with the Federal Information Security Modernization Act (FISMA) of 2014.

The vendor is mLINQS, which is a cloud service provider (CSP) with headquarters in Fairfax, Virginia.

TTRS is composed of 3 portals. These 3 portals are the Expense Manager, Approver Portal, and Employee Portal. Privileged activities occur in the Expense Manager; single sign on (SSO) is enforced on both Expense Manager and Approver Portal. Regarding the Employee Portal, SSO is offered, but not enforced, along with password-based authentication. The Employee Portal requires password-based authentication due to business requirements of a worldwide user community and access for former DOJ employees; the latter technically being non-DOJ users. The employee portal is a way for employees to view entitlements, upload receipts and invoices, and submit claims for their relocations or taxable travel assignments.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	The Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq. 5 U.S.C. Chapter 57-Travel, Transportation, and Subsistence U.S. Code Title 26-Internal Revenue Code
Executive Order	

[1] FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. See https://www.fedramp.gov/.

Federal regulation	41 C.F.R. §§ 300-304-Federal Travel Regulation System 41 C.F.R. Part 300-70-Federal Travel Regulation System, Agency Reporting Requirements 26 C.F.R. § 31.3402(g)-1 Supplemental wage payments
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	Publication 15 (2024), (Circular E), Employer's Tax Guide | Internal Revenue Service (irs.gov)

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*A, B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	*A, B, C and D*	Names of DOJ employees and family members
Date of birth or age	X	B, C and D	Some Bureaus may choose to not include dependent ages (but, not DOB). This would be for relocating employees' dependents.
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	Full. Truncated or masked when W2s are created. System has privileged access for control of SSN to only those administrative personnel who require access for processing taxable travel payments.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Tax Identification Number (TIN)	X	A	System has privileged access for control of TIN to only those administrative personnel who require access for processing taxable travel payments.
Driver's license			
Alien registration number			
Passport number	X	B, C and D	Family and dependents members in some instances
Mother's maiden name			
Vehicle identifiers	X	B, C and D	Family and dependents members in some instances
Personal mailing address	X	B, C and D	Family and dependents members in some instances
Personal e-mail address	X	B, C and D	Family and dependents members in some instances
Personal phone number	X	B, C and D	Family and dependents members in some instances
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B and C	DOJ employment information, and, if spouse is a federal employee, information may be captured for spouse relocation by DOJ or other federal agency
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices		A	Mobile phone number
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records	X	A	Supporting details documenting reimbursement of travel and relocation payments.
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	System audit includes Row title.
- **User passwords/codes**	X	A	System audit includes Row title.
- **IP address**	X	A	System audit includes Row title.
- **Date/time of access**	X	A	System audit includes Row title.
- **Queries run**			
- **Contents of files**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Contracting information with regard to GSA Government-wide Transportation Management contracts for shipping, moving, and storing of household goods and privately owned vehicles.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Internal processing
DOJ Components			X	System management and processing of tax documents
Federal entities	X	X		Tax information to IRS GSA-required transportation audit logs for all shipment of household goods GSA statutory and regulatory reporting per Title 5 5707 and CFR 41 300.
State, local, tribal gov't entities	X	X		Tax information to state revenue tax departments
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A. Please note, the Employee Portal provides access for former DOJ employees which are technically non-DOJ users. The employee portal is a way for DOJ employees and former DOJ employees to view entitlements, upload receipts and invoices, and submit claims for their relocations or taxable travel assignments.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of

Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

TTRS provides notice to users when logging into the employee and approver portals. The front page of the sign in requires users to "Accept" and includes the following privacy statement.

> This information system could be storing or processing U.S. Government information. You must conduct only authorized business on the system. Your level of access to systems and networks owned by mLINQS is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify your agency Security Office and application administrator. You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a mLINQS employee should never ask you to reveal them. You must follow proper logon/logoff procedures. You must manually logon to your session; do not store your password locally on your system or utilize any automated logon capabilities. You must promptly logoff when session access is no longer needed. If a logoff function is unavailable, you must close your browser. Never leave your computer unattended while logged into the system.
>
> You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to mLINQS systems and networks to your agency Security Office and application administrator. You must not establish any unauthorized interfaces between systems, networks, and applications owned by mLINQS. Your access to systems and networks owned by mLINQS is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable mLINQS system maintains individual Privacy Act information. Your access to mLINQS systems constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable state and federal laws. You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation. You must not process U.S. classified national security information on the system. You must not browse, search or reveal information hosted by mLINQS except in accordance with that which is required to perform your legitimate tasks or assigned duties. You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.
>
> You must ensure that Web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.2 (or higher). SSL and TLS must use a minimum of 128-bit encryption. You must ensure that your web browser is configured to warn about invalid site certificates. You must ensure that web browsers warn if the user is changing between secure and non-secure mode. You must ensure that your web browser window used to access systems owned by mLINQS is closed before navigating to other sites/domains. You must ensure that your web browser checks for a certificate revocation from a publisher. You must ensure that your web browser checks for server certificate revocation. You must ensure that web browser checks for signatures on downloaded files. You must ensure that web browser empties/deletes temporary Internet files when the browser is closed. By your signature or electronic acceptance (such as by clicking an acceptance button on the screen) you must agree to these

rules. You understand that any person who obtains information from a computer connected to the Internet in violation of computer-use restrictions from their employer is in violation of the Computer Fraud and Abuse Act. You agree to contact your agency Security Office or application administrator if you do not understand any of these rules.

Accept Decline

Employees accessing mLINQS expense management portal receive the following notice:

"Your access to systems and networks owned by mLINQS is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable mLINQS system maintains individual Privacy Act information. Your access to mLINQS systems constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable state and federal laws". Those accessing the approver and employee portals receive the following notice: "This is a U.S. Government computer system. U.S. Government computer systems are provided for the processing of Official U.S. Government information only. All data contained on U.S. Government computer systems is owned by the U.S. Government and may, for the purpose of protecting the rights and property of the U.S. Government, be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. There is no right of privacy in this system. System personnel may give to law enforcement officials any potential evidence of crime found on U.S. Government computer systems. Use of this system by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, recording, reading, copying, or capturing and disclosure. This system contains information protected under the provisions of the privacy act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed must be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary action, a fine of up to $5,000, or both.

In addition, the following SORNs provide general notice to the public: DOJ-001, Accounting Systems for the Department of Justice (69 FR 31406) (6-03-2004) -04-12578.pdf (govinfo.gov), and DOJ-002, DOJ Information System and Network Activity and Access Records (86 FR 37188) (7-14-2021). 04-12578.pdf (govinfo.gov)

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

TTRS is a system that allows DOJ to process tax withholdings on the employee's behalf, payments to tax authorities, and tax reports to employees and tax authorities. This is a tax system similar to a payroll system of withholdings from payments to employees or on employee's behalf, payments to tax authorities, and tax reporting to employees and tax authorities. Employees must validate all information within the system with respect to dependents and entitlements is correct. Additionally, they must sign each reimbursement request certifying they are entitled to reimbursement based upon dependents if they so exist.

Employees may request review of their tax information reported to the taxing authorities to their respective Bureau, even after they have signed and received payment associated with individual

reimbursements. Such requests are reviewed and sent to the tax processing team for validation of accurate reporting according to the relocation records, Federal Travel Regulations, and tax authorities' requirements and regulations. If any necessary changes are identified, the records will be amended. Information shared with GSA is compliant with statute and federal regulations and does not include individual information. Without the necessary information and certifications of accuracy, the government will not be able to process employee reimbursement or properly execute the required taxation and reporting.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Annual tax documents (*e.g.,* W2s) and payment vouchers are provided to employees by component, accessed through web-based portals of the system, or may be requested from the component servicing the employee's relocation. Employees may request what PII is in the system regarding themselves and dependents from the Bureau responsible for their relocation. Employee portals are only for entering information related to entitlement reimbursements. If information regarding their record is incorrect, the authorized administrator of their relocation within their Bureau must make those updates to the system of record, e.g., SSN.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. =Provide date of most recent Authorization to Operate (ATO):** ATO effective June 22, 2022, through June 21, 2025. **If an ATO has not been completed, but is underway, provide status or expected completion date: N/A** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** N/A.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and**

	consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: The assigned security category is Moderate. The mLINQs Host Service (MHS) and TTRS assigned the Moderate categorization based upon the information types that are input, stored, processed and or output. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. • A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** As implemented in the TTRS System Security Plan (SSP), Finance Staff employs the following processes to monitor security control compliance by Finance Staff and mLINQS cloud service provider (CSP) on an ongoing basis: 1. Continuous monitoring of MHS FedRAMP package in Office of Management and Budget (OMB) MAX portal on a monthly basis to identify and track vulnerabilities that impact DOJ; 2. Communication with mLINQS security personnel, as necessary; and 3. Continuous monitoring of TTRS security controls per DOJ Order 0904.
X	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Audit and Accountability (AU) control requirements are defined in DOJ Order 0904 and DOJ Cybersecurity Standard. Specifically: DOJ Cybersecurity Standard, AU-06 Audit Record Review, Analysis, and Reporting states: a. Review and analyze system audit records weekly and maintain documented records of what events were reviewed to demonstrate completeness of the review for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; b. Report findings to the System Owner, Information System Security Officer, or incident response personnel, as appropriate; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

	d. The TSG TTRS Support team reviews and analyzes all the events records captured in the TTRS application. The team conducts weekly review of the audit logs for indications of inappropriate or unusual activity. The audit log events reviewed include unsuccessful logon attempts; account management events; unsuccessful accesses to objects; policy and configuration changes; privileged activities; process tracking; and system events. e. The team reports findings to the Designated Signing Official or the TSG System Administrator. JMD Finance Staff developed an RPA bot to assist in the automated review of user activities within the TTRS environment. f. FSCS created a Weekly Audit Logs SOP.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Yes.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: No additional training is required for this system.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Only role-based access is permitted and PII is restricted to only those with a need to know. There is no data shown in the data element for individuals who have not been assigned a role allowing them access to certain PII.

mLINQS protects MHS information at rest using Azure SAKs provided by Microsoft Azure. The SAK is a secret key that is used to manage database encryption and encryption of storage.

All mLINQS users with access to the Azure DevOps and ServiceDesk application have obtained at least one Public Trust clearance. For additional data protection, Microsoft Data Loss Prevention (DLP) is implemented and configured to alert the security officer in real-time when it detects sensitive PII stored on corporate SharePoint sites, Microsoft Teams sites, OneDrive, or email.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Information in the system is retained based upon National Archives and Records Administration's (NARA) travel documents requirements GRS 1.1, item 010 and IRS Publication 15, (Circular E), Employer's Tax Guide.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DOJ-001, *Accounting Systems for the Department of Justice* (69 FR 31406) (6-03-2004) -04-12578.pdf (govinfo.gov).

JUSTICE/DOJ-002, *DOJ Information System and Network Activity and Access Records* (86 FR 37188) (7-14-2021) . 04-12578.pdf (govinfo.gov).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Data in the system will be retained in accordance with the applicable NARA-approved record retention schedules. Notice is provided to users as described in Section 5.1.

Access to data in the system is limited to privileged/authorized users who are certified annually per AC-02 from DOJ Cybersecurity/DOJ Order 0904. Controls, such as partitioning and limited user-

specific roles for PII are used to protect the data. Controls are put in place via privileged roles and user roles to accomplish separation of duties. User roles are further divided based on required access, such as Counselor, TSG Auditor, Funds Certifier, Employee, OBD Relocation Supervisor, and OBD Accounting Tech. Each user role has unique, limited access and no one role has access that overlaps with another role.

No data is collected which is not required by authorities for taxes and travel, i.e., IRS and GSA. Retention is not a discretion of DOJ; DOJ only retains up to the minimum required time. IRS (and other tax authorities) require reporting of taxable income, withholdings, and associated identification data. This is the same information required by the IRS of HR departments and associated contractors completing the HR tax requirements for DOJ. Shipping information is provided to contractors of GSA, including employee's information such as address for relocating household goods and personal vehicles from one duty station to another or storage facilities.

Only required information is collected and shared. For example, it is impossible for an employee to refuse to opt out of giving SSN or address. The SSN is the identifier used by IRS and address must be included for the moving van to pick up household goods. Any refusal to give this information would result in non-compliance with federal statutes or regulations, or the inability of the employee to complete the relocation.

There are various layers of security controls in place to protect and access data. Policies, standards, and standard specifications have been implemented that are designed and align with the National Institute of Standards and Technology (NIST) 800-53 frameworks[2]. Controls for physical / environmental security, access, operations, organization, network, system security (masking, encryption, secure coding practices and vulnerability management), incident response, Disaster Recovery / Business Continuity and compliance add levels of security. A "defense in depth" strategy is employed, applying multiple levels of security controls that ensure the confidentiality, integrity, and availability of personal data. These include Data Security – personal information is protected in transit outside of DOJ and mLINQs networks using secure encryption protocols. TTRS is developed and maintained per mLINQs secure coding standards. Comprehensive Access Controls - access to data, applications and systems is granted only once it is approved and based on minimum necessary privilege.

[2] See: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.