U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: BTFA ServiceNow System (BTFASNS)
Bureau/Office: Bureau of Trust Funds Administration (BTFA)
Date: September 30, 2021
Point of Contact:
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: btfa_privacy@btfa.gov
Phone: (505) 816-1645
Address: 4400 Masthead St. NE, Albuquerque, New Mexico 87109

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Bureau of Trust Funds Administration ServiceNow System (BTFASNS) is an enterprise Information Technology (IT) service management solution software platform that supports IT service management and automates common business processes. The software as a service (SaaS) platform contains a number of modular applications that varies by instance and user. The BTFASNS Service Automation Government Cloud Suite is a is a stand-alone system that is

physically and logically separated from the ServiceNow Public Cloud offering. It is hosted in two data centers that house infrastructure dedicated to the Government Community Cloud. The network architecture and access controls separate it from the ServiceNow Public Cloud. The single-tenant environment adds an additional layer of logical separation between instances. Federal customers share a hardware platform (no virtualization), but access entirely separate individual instances of the ServiceNow platform located in the dedicated federal data center cages. Each individual instance connects to a database only accessible by that specific instance.

The BTFASNS helps BTFA create and respond to IT-related tickets, is used to monitor controls related Trust risk and compliance issues in support of BTFA's lines of business, including Business, Financial, and IT services, and provides technical support for the BTFA Innotrust Trust Funds Accounting System (TFAS) Portal.

BTFASNS is a FedRAMP certified cloud service provider solution that allows organizations to quickly build new apps directly into ServiceNow leveraging existing platform services, applications and integrations to support IT service automation, resource management and shared support services. The application pulls customer contact information from Active Directory (AD) and facilitates single sign-on (SSO). The following are integrated with BTFASNS:

- Service Management Suite for users that are assigned tickets and work the tickets for use by the Office of Information Resources (OIR) and the Trust Funds Accounting System (TFAS) Command Center Staff;
- ServiceWatch Mapping (Discovery and Service Mapping);
- ServiceNow Orchestration (Password user and Client Distribution);
- Performance Analytics;
- Approver Licenses to allow BTFA Supervisors and Managers to approve workflow actions for employees and contractor staff, such as procurement of IT resources, onboarding and off boarding, IT Access requests, shared drives requests; and
- Governance, Risk, and Compliance (GRC) now called, Integrated Risk Management (IRM) managed by the Office of Trust, Risk, Evaluation, and Compliance (OTREC).

Tickets and requests are accessible by authorized users in the self-service portal. All BTFASNS information and processes are located off premises in the cloud provider's FedRAMP certified data centers. BTFASNS does not request for sensitive personally identifiable information PII. User identity information is originally collected by DOI Access via the onboarding process. The data in the AD is necessary for identity management and required under Federal mandates. The AD account information for user access is through the Enterprise AD, which is assessed separately in the DOI's Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment (PIA) and may be viewed at https://www.doi.gov/privacy/pia. AD user account information includes

names, passwords, and login time, data, and locality, and is used to authenticate user access and actions within EHI.

C. What is the legal authority?

5 U.S.C. 301, Departmental regulations; Homeland Security Presidential Directive 12 (HSPD-2); the Office of Management and Budget (OMB) Directive M-12-18, Managing Government Records; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, Streamlining Service Delivery and Improving Customer Service; 25 U.S.C. 116, 117a, 117b, 117c, 118, 119, 120, 121, 151, 159, 161a, 162a; 4011, 4043(b)(2)(B), Public Law 93–638 Self-Governance Compacts; 25 U.S.C. 5363(d)(1); 25 CFR 1000.350; 25 CFR 1000.355; and 25 CFR 1000.365.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☒ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000910, 010-000000911; BTFASN System Security and Privacy Plan.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	N/A	N/A	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

BTFASNS is not an official Privacy Act system of records but it provides support to other systems of records. This system supports IT service management and automates common business processes for various lines of business within BTFA. Therefore, these records are under the control and ownership of each system owner, information owner, or Privacy Act system manager and may be covered under numerous government-wide, DOI, or BTFA SORNs including the OS-02, Individual Indian Money (IIM) Trust Funds when creating or processing work tickets and service request tickets; DOI-58, Employee Administrative Records for asset/ property management of Government Furnished Equipment; DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) covering records related to AD for BTFA authorized users to access the system. The SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Other: *Specify the PII collected.*

PII is limited to official work contact information, such as work email address and phone numbers. Personal contact information may be provided by employees who are working remotely; typically, personal cell and home telephone numbers as an alternative method for authorized users to contact the employee to resolve a ticket. PII is not collected when creating and processing a work ticket or service request ticket, however, PII may be

inadvertently provided by an employee when submitting a work ticket or service request ticket. The BTFA IT help desk support staff require a username for AD authentication to access the system which contains user name, display name, and are populated by the DOI Access system.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe.* DOI authorized contractors, contracted tribal employees, and external auditors.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe:* Data is pulled from AD twice a day to ensure user data is accurate and current. User initiated processes may automatically push data into BTFASNS to fulfill service requests.
☐ Other: *Describe.*

D. What is the intended use of the PII collected?

The use of employee contact information is obtained from AD and used to create and respond to work tickets and service request tickets. Personal contact information may be provided by employees who are working remotely. Typically, personal cell and home telephone numbers are used as an alternative method for authorized users to contact the employee, to resolve a work ticket or service request ticket.

BTFASNS does not collect PII from individuals to process work tickets or service request tickets; however, PII may be inadvertently provided by an employee when submitting a work ticket or service request ticket. Depending on the user, BTFASNS pulls different types of information about the IT system, software, or technology-related information, or from the user,

in order to best determine how to resolve an issue for a work ticket or service request. BTFASNS authorized users may mistakenly collect sensitive PII to support TFAS functions.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Data is used by BTFA IT help desk support staff to create work or incident tickets, problem tickets, and service request tickets. TFAS data is shared with TFAS authorized users and is not maintained in this system.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Data may be shared with DOI-CIRC to respond to privacy and security incidents.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Data collected for security and privacy incidents may be reported by DOI-CIRC to the Department of Homeland Security US-CERT. Information may be shared with other Federal law enforcement agencies for investigative purposes.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Data may be shared with BTFA contractors that provide support to the BTFASNS in responding to and resolving work tickets or services requests tickets.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Data is shared with external auditors or the Inspectors General (IG) in the performance of annual or financial audits.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

BTFA authorized users submitting work tickets and service requests ticket may choose to voluntarily provide official or personal contact information. Personal contact information may be voluntarily provided as an alternative contact method for individuals working remotely. Not

providing contact information may impede or delay response or resolution of the employee's issue or service request.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this PIA. Some work tickets or service request tickets, in the ticket or attachments, may mistakenly include PII that are covered by DOI-58, Employee Administrative Records, DOI-47, HSPD-12: Logical Security Files (EACS), or by the OS-02, IIM Trust Funds SORN. DOI and BTFA SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

Authorized users are presented with a DOI security warning banner that informs them they that they are accessing a DOI system, are subject to being monitored and there is no expectation of privacy during use of the BTFASNS.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Tickets and information may be retrieved by name, incident identification number, reference number, and/or work email address. User AD information is retrieved by name, username, and AD group names. Retrieval occurs when resetting passwords, to change permissions, transfer or move accounts, and add/remove workstations; and, may also be retrieved in working with service requests.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports will be produced to track BTFASNS work tickets and service requests tickets. The tickets, and request history, is viewed for customers when they submit a request for assistance. In addition, IT help desk support staff can see the details of any assigned government furnished computer equipment. Performance is tracked for service level records by IT help desk support

personnel. Audit logs track user activity in accordance with DOI logging requirements. The logged information is used for investigative actions associated with cyber security and privacy incidents that are reported to DOI-CIRC or other internal organizations, as necessary.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

All data contained in BTFASNS is associated with existing DOI and BTFA records. Data is kept current through daily updates from the AD and asset inventories are updated annually as required by annual ongoing authorization. User information that is obtained from the DOI enterprise AD are kept current through procedures managed by the Department. Information provided by individuals is assumed to be accurate at the time it is used by BTFASNS. All the BTFASNS information and processes are located off premises in the cloud provider's FedRAMP certified data centers.

B. How will data be checked for completeness?

Data is checked for completeness by the employee or authorized user providing the data and is crossed-referenced with existing DOI or BTFA databases, such as AD. Data is kept current by daily updates from the AD and asset inventories that are updated annually, as required by annual ongoing authorization. User information that is obtained from the DOI enterprise AD are kept current through procedures managed by the Department.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data is kept current and the information is verified by the employee as work tickets and service requests tickets are submitted. User data is kept current by daily updates from the AD and asset inventories that are updated annually as required by annual ongoing authorization. User information that is obtained from the DOI enterprise AD are kept current through procedures managed by the Department.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

The BTFASNS records are covered by the National Archives and Records Administration (NARA) approved Departmental Records Schedule, DAA-0048-2013-0001-0013, System Maintenance and Use Files. Records are cut-off when superseded or obsolete, and are destroyed no later than three years after cut-off. Work tickets and service requests tickets including those with PII (if attached at the time the ticket was created) are destroyed three years after the ticket is

resolved, or when no longer needed for business use. BTFASNS maintains historical work tickets and service request to analyze recurring problems and records.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Data and information associated with the BTFASNS system are retained under the appropriate NARA approved records retention and disposition schedules. Electronic records will be deleted and temporary records will be shredded or pulped. Backup tapes are reinitialized and reused. The BTFA exit clearance process documents the steps and procedures used to remove or archive information when employees or contractors leave BTFA. System administrators dispose of paper records by shredding or pulping and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are risks to the privacy of individuals due to the information received by the BTFASNS system. The risk is mitigated through security and privacy controls to protect the system and data. The principle of least privilege is observed during all phases of the information lifecycle. The potential privacy risks identified include inadvertent disclosure, unauthorized access, surveillance or theft of data. Any unauthorized disclosure may reveal details of an individual's IP address, contact information and service request history. All data is stored and maintained in secure systems and is protected from unauthorized access by firewalls, intrusion detection systems, antivirus and the AD domain environment. User activity is monitored and logged to ensure only appropriate use of the system and data.

To mitigate the insider threat, BTFASNS data is protected by access controls, including two-factor authentication, least privilege principles, and restricted access is limited to authorized users. Employees are required to complete annual Information Management and Technology (IMT) Awareness Training, which includes privacy and security training, and affirm the BTFA Rules of Behavior. Those with access to PII are required to also complete mandatory role-based privacy training annually. BTFA computers are secured and monthly scans are conducted in accordance with the BTFA Continuous Monitoring Plan.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The BTFASNS is provided and hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with Federal Information Security Modernization Act of 2014 (FISMA). The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and National Institute of Standards and Technology (NIST) guidelines. The cloud service provider is subject to all the

Federal legal and policy requirements for safeguarding Federal information, and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that the system may collect, store or share more information than necessary, or the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Access to data is restricted and authorized personnel only retrieve and process service requests as authorized and necessary to perform official functions. Data maintained is limited to the minimal amount of data needed to meet Federal records requirements and the applicable retention schedules.

There may be risks that some data may not be appropriate to transfer to other agencies or AD, or that contractors may not handle information according to DOI policy. A system security and privacy plan was completed to address security controls and safeguards for the BTFASNS Cloud system. Controls are outlined in the BTFASNS Security and Privacy Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, and includes the requirements for awareness and role-based training, encryption, and maintaining data in secure facilities, among others. Backups are stored and encrypted within SQL server file system. BTFASNS implements audit logging mechanisms for the information systems and its applications. Splunk is utilized for near real-time audit logging and reporting as the centralized Security Information and Event Management solution for security monitoring, advanced threat detection, insider threat analysis, incident investigation and forensics, incident response planning, compliance management, and fraud detection. Audit logging is utilized to assess BTFASNS security posture in the identification of potential incidents or compromised systems by monitoring for vulnerabilities that lead to breaches. The Splunk solution is utilized for account monitoring by maintaining a consistent and accurate monitoring process of account and data access. In addition, Splunk monitors and logs for compliance purposes by establishing a historical baseline and understanding the scope and data in BTFASNS infrastructure and comparing log information for anomalies. Web application auditing and logging takes place within the application to establish an audit trail of events taking place within the BTFASNS. Splunk is further utilized to automatically pull the logging information from the audit logs created by the application into the Splunk centralized solution for analysis. Risk assessments have been conducted and includes the likelihood and magnitude of harm resulting from unauthorized events such as unauthorized access, use, disclosure, disruption, modification and destruction of data. The risk assessment results are documented in a formal security assessment report (SAR).

There is some privacy risk associated with lack of notice for the use of employee or contractor information associated with the BTFASNS. Authorized users have the opportunity to decline to provide their information, or the option to not use the system when they submit a work ticket or service request ticket. This risk is mitigated by the privacy notice provided during the hiring and onboarding process, this PIA and related SORNs. The privacy notice describes the ways individuals' information may be used, shared and disseminated and provides prospective employees the opportunity to decline to provide personal information.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The data is used to create or track work tickets and service requests tickets, or to follow up with individuals if more information is needed about their submitted ticket. Authorized user identity information is originally collected by DOI Access via the onboarding process. The BTFASNS uses data in the DOI AD and is necessary for identity management and required under Federal mandates. The application pulls customer contact information from AD and facilitates single sign-on (SSO). BTFASNS information and processes are located off premises in the cloud provider's FedRAMP certified data centers.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe:*

Auditors may have access to data associated with annual reviews or audits. Authorized users and contractors will have access to their own information, and in some cases a limited subset of other users' information based on the BTFA mission, system, and for application management needs. Contractors working for BTFA fall into the same category as "All Users."

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Authorized users have access to create and amend their assigned tickets or service requests. End users have access to their own tickets and service requests. User access is based on the role and duties of the employee (contractor) and is limited to authorized personnel who have a need to access the data in the performance of their official duties. Authorized users are trained and required to follow established internal security protocols, and must complete annual security, privacy, and records management training, and sign the BTFA Rules of Behavior.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The appropriate contract clauses were included in the contracts associated with BTFASNS.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

Routine file maintenance audit records are maintained, that identify when account asset, name/address information is created, maintained/changed and deleted. System logs capture date and time users log in and any changes that are initiated. All user activity is audited as part of the security monitoring and management of user accounts and can be reviewed by Security Personnel and all user actions taken on BTFA IT systems are audited. The information includes items such as: failed login/access attempts, changes in user permissions, etc., that are associated with user authentication.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The BTFASNS logs every change to the record(s) and system by capturing the name, login ID, timestamp, and what fields were changed. All actions by authorized users can be reviewed for auditing purposes. Audit reports are customizable and may include, but are not limited to, unique applicant ID logon/logoff timestamps, data accessed and or/modified; and permission changes.

M. What controls will be used to prevent unauthorized monitoring?

Access is limited to authorized personnel who have a need to access the data in the performance of their official duties. All changes are logged by BTFASNS and audit logs are used to prevent unauthorized monitoring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges

☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe:*

BTFASNS is maintained at FedRAMP certified data centers with all required physical controls.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Deputy Associate Chief Information Officer (DACIO) is the Information System Owner (ISO) for BTFASNS. The ISO, Information System Security Officer (ISSO) and the BTFA Associate Privacy Officer (APO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in accordance with Federal laws and policies for the data managed, used, and stored in BTFASNS. The System Manager in consultation with the BTFA APO is responsible for protecting the privacy rights of the employees for the information collected in BTFASNS.

The BTFASNS vendor and cloud service providers are also responsible for the protection of PII, incident reporting, and other privacy controls to ensure adequate safeguards are implemented in accordance with the appropriate Federal laws, regulations, and Departmental policies.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ISO and ISSO are responsible for oversight and management of the BTFASNS security and privacy controls. All authorized users are responsible for immediately reporting suspected loss, compromise, unauthorized access or disclosure of PII from the system in accordance with the rules of behavior and DOI policy. The BTFA APO and the ISSO coordinates the investigation of reported violations from users. They are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.