Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

Privacy Impact Assessment
for
Spartan

Issued by:
Adam Siple, Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: February 17, 2023

(May 2019 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.)

Spartan is a system for the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), that serves as the case management system and database for creating, tracking, and collecting investigative information and inspections in support of ATF's regulatory, strategic, law enforcement mission, program initiatives, and tactical field activities. This effort will streamline information access for different ATF components by bringing together interconnected, but separate operational workstreams.

ATF Spartan is a customized system built using PEGA[1], serving as a single solution business tool with state-of-the-art capabilities for criminal enforcement, industry operations, and intelligence missions. The Spartan user base is expected to grow to approximately 4,900 Industry Operations Investigators, Special Agents, and Intelligence Research Specialists by the end of Fiscal Year 2023. The Spartan application is housed in the ATF Amazon Web Services GovCloud[2] Federal Risk and Authorization Management Program ("FedRAMP")[3] complaint environment using infrastructure as a service.[4] Spartan will automate process flows for tasking, report reviews and approvals, evidence management, and criminal intelligence analysis.

ATF prepared a Privacy Impact Assessment for Spartan because ATF collects information in identifiable form about individuals during the course of an investigation. PII gathered throughout the course of investigations or inspections, and therefore implicated in Spartan, can include, but is not limited to name, addresses, Social Security numbers (SSN), email addresses, and social media handles.

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.

---

[1] PEGA, or Pegasystems Inc. is an American software company based in Cambridge, Massachusetts. PEGA provides a Business Process Management tool, which is developed on Java and uses object-oriented programming and Java concepts that allow users to execute changes quickly.

[2] Amazon Web Services is a Cloud Service Provider (CSP) that offers Cloud Service Offerings (CSOs). As a CSP, Amazon Web Services follows the FedRAMP process to get its CSOs authorized for Federal use.

[3] The Federal Risk and Authorization Management Program **(**FedRAMP) refers to the government program that strives to standardize security assessments and authorization for cloud products and services used by U.S. federal agencies. The goal is to make sure federal data is consistently protected at a high level in the cloud.

[4] Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. IaaS is one of the three main categories of cloud computing services, alongside software as a service ("SaaS") and platform as a service ("PaaS").

Spartan is ATF's modernized case management system, combining the business areas of industry operations (IO), criminal enforcement (CE), and intelligence into a single system for both records management and information sharing. As a unified system, Spartan provides enhanced communications and data, to assist with the deconfliction of data between the IO and CE business areas. Spartan contains PII gathered throughout the course of investigations or inspections, and can include, but is not limited to names, addresses, Social Security numbers (SSN), email addresses, and social media handles.

Spartan is designed to include business process workflows, which will allow coordination between offices and operational workstreams and retain the integrity of ATF records management data. This will increase accountability in regard to auditing, managing, and documenting the probable cause for administratively seized property. Spartan's auditing capabilities regarding the movement of property will now be contained in one system, and probable cause statements with legal justification for seizure of the property will be linked directly to the property itself. This will assist legal counsel's review of probable cause information over the current legacy N-Force application[5]. In time, as Spartan is deployed across the bureau, the legacy application will stand down for all new cases, except those from the National Instant Criminal Background Check System (NICS[6]) and will remain open only to facilitate Spartan connections to N-Force.

Spartan is accessible via a web-browser or mobile device through ATF's internal network via Justice Unified Telecommunications Network (JUTNET), and a Virtual Private Network (VPN) for mobile device access. Users accessing the Spartan system must first authenticate to the ATF network using a government issued Personal Identity Verification (PIV)[7] Card. The user's PIV credentials are supported through the network to the application.

As noted above, Spartan is the investigative case management platform created to support investigations conducted by ATF personnel, including but not limited to special agents, investigators, and intelligence research specialists, and, technically speaking, consists of the following:

- Pega: A Java Enterprise Edition (EE)-compliant enterprise application that requires an application and database server, the Pega platform is a business process management system. For Java EE compliance the application must be written according to Java enterprise specifications assuring that the application will be able to be deployed and executed on any Java Enterprise edition application server.

- Documentum: Documentum is a content management software tool for storing and managing file attachments such as pictures, videos, and documents. A Documentum installation typically consists of one or more repositories, content servers that access the repositories, and clients that access the repositories through the Content Servers. Content server software manages the repository and provides content management capabilities. The repository consists of three main

[5]N-Force is a computer-based case management system that supports ATF's law enforcement operations by providing automated collection, dissemination, management, and analysis of investigative data.
[6] National Instant Criminal Background Check System (NICS) is an FBI system – PIA: https://www.fbi.gov/file-repository/pia-nics.pdf/view
[7] Personal Identity Verification (PIV) card is an identification card issued by a federal agency that contains a computer chip, which allows it to receive, store, recall, and send information in a secure method.

components: a file store containing the content assets, attribute tables within a relational database, and full-text indexes. The file store resides outside of ATF's GovCloud on a NetApp appliance at the Seattle Equinix facility.

Spartan is utilized by ATF's Industry Operations Investigators (IOI) and Joint Support & Operations Center (JSOC) personnel to conduct the following functions:

- Firearms Application Inspections (FAI):
    - Application inspections are conducted to ensure that applicants are familiar with the Gun Control Act and other federal firearms laws[8] and regulations;
- Explosives Application Inspections (EAI), including Collateral sites[9]:
    - Inspections of applicants for explosives licenses or permits, to ensure that applicants are knowledgeable of the applicable federal explosive laws and regulations;
- Explosives Compliance Inspections (ECI):
    - Compliance inspections of current license and permit holders ("licensees") to ensure that they are following federal explosives laws and regulations;
- Firearms Compliance Inspections (FCI):
    - Compliance inspections are conducted to ensure that FFLs are obeying federal firearms laws and regulations;
- Suspicious Activity Reports to Crime Gun Intelligence Centers (CGICs):
    - Crime Gun Intelligence Centers serve as intelligence hubs and coordination centers for local, state and federal responses to mass shootings and other major crimes involving firearms;
- Referrals to outside agencies:
    - Information that is found to be applicable for external agencies is referred by CGIC and JSOC; and
- Wanted Persons (Joint Support Operations Center (JSOC)):
    - JSOC provides the core situational awareness capability for ATF. This is accomplished by collecting and disseminating information to facilitate planning and responses to incidents that impact ATF's mission.

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

[8] The National Firearms Act, Title 26 U.S.C. Chapter 53; The Arms Export Control Act of 1976, Title 22 U.S.C. § 2778.)
[9] Collateral sites are explosives sites which Industry Operations sends personnel from other ATF divisions or offices to inspect. For example: Industry Operations Investigator inspects a business with explosives magazines in 3 different states. These would be collateral sites.

X	Statute	• 18 U.S.C., chapter 40 (related to explosives), chapter 44 (related to firearms), chapter 59 (related to liquor trafficking), and chapter 114 (related to trafficking in contraband cigarettes); • Chapter 53 of the Internal Revenue Code of 1986, 26 U.S.C. chapter 53 (related to certain firearms and destructive devices); • Chapters 61 through 80, inclusive, of the Internal Revenue Code of 1986, 26 U.S.C. chapters 61–80, insofar as they relate to activities administered and enforced with respect to chapter 53 of the Internal Revenue Code of 1986, 26 U.S.C. chapter 53; • 18 U.S.C. §§ 1952, 3667, insofar as they relate to liquor trafficking; • 49 U.S.C. § 80303 and 80304, insofar as they relate to contraband described in section 80302(a)(2) or 80302(a)(5); and • 18 U.S.C. §§ 1956–1957, insofar as they involve violations of: o 18 U.S.C. § 844(f) or (i) (relating to explosives or arson), o 18 U.S.C. § 922(l) (relating to the illegal importation of firearms), o 18 U.S.C. § 924(n) (relating to illegal firearms trafficking), o 18 U.S.C. § 1952 (relating to traveling in interstate commerce in aid of racketeering enterprises insofar as they concern liquor on which Federal excise tax has not been paid); o 18 U.S.C. §§ 2341–2346, 2341–2346 (trafficking in contraband cigarettes); • (vi) Section 38 of the Arms Export Control Act, as added by Public Law 94-329, section 212(a)(1), as amended, 22 U.S.C. § 2778 (relating to the importation of items on the U.S. Munitions Import List)
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	

	Other (summarize and provide copy of relevant portion)	

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
Name	X	A, B C & D	
Date of birth or age	X	C & D	
Place of birth	X	C & D	
Gender	X	C & D	
Race, ethnicity or citizenship	X	C & D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	
Tax Identification Number (TIN)	X	C & D	
Driver's license	X	C & D	
Alien registration number	X	C & D	Alien registration number, Visa information and residency status.
Passport number	X	C & D	Passport number and country of issue.
FBI Number	X	C & D	
Mother's maiden name			
Unique Personal Identification Number (UPIN)			
Vehicle identifiers	X	C & D	
Personal address	X	C & D	
Personal e-mail address	X	C & D	
Personal phone number	X	C & D	
Business address	X	C & D	
Business e-mail address	X	A, B, C, & D	
Business phone number	X	A, B, C & D	

(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
Personal Social Media account(s)	X	C & D	Personal Social Media accounts, consistent with applicable law.
Business Social Media Account(s)	X	C & D	Business related Social Media accounts, consistent with applicable law.
Medical records number	X	C & D	Possibility of medical records for prisoners going to US Marshal Service (USMS).
Medical notes or other medical or health information	X	C & D	Possibility of medical records for prisoners going to USMS.
Financial account information	X	C & D	Financial account information relating to bank accounts, credit cards, income, taxpayer information.
Applicant information	X	C & D	Federal Firearms Licensee applicate information, or if included as part of an investigation.
Education records	X	C & D	Is possible if included in an investigation.
Military status or other information	X	C & D	Is possible if included in an investigation.
Employment status, history, or similar information	X	C & D	Employment status for FFL employees, or if included as part of an investigation.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	Is possible if included in an investigation.
Certificates			
Legal documents	X	A, B, C & D	

(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
Device identifiers, e.g., mobile devices	X	C & D	Mobile device information can include equipment serial number (ESN)[10], make, model, international mobile subscriber identity (IMSI) [11]and international mobile station equipment identity (IMEI). [12]
Web uniform resource locator(s)			
Foreign activities	X	A, B, C & D	Information concerning individuals and law enforcement related to ATF investigations that involve non-US territories.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Criminal history, arrest information, documentation of suspected violations of law, and criminal charges.
Juvenile criminal records information	X	C & D	
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	Information related to civil, criminal, and administrative violations.
Whistleblower, e.g., tip, complaint or referral			
Grand jury information	X	C & D	Grand jury information.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, & D	Witness statements, contact details
Procurement/contracting records			
Proprietary or business information	X	C & D	Import/export
Location information, including continuous or intermittent location tracking capabilities	X	C & D	Location tracking data
Biometric data:			

[10] ESN Electronic serial numbers (ESNs) were created by the U.S. Federal Communications Commission (FCC) to uniquely identify mobile devices,
[11] IMSI (International Mobile Subscriber Identity) is a code used by the phone company to identify the SIM on the mobile network.
[12] IMEI (International Mobile Station Equipment Identity) is an international "Serial number" for your phone (device itself) to properly identify it on the carriers' network.

(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
- **Photographs or photographic identifiers**	X	C & D	
- **Video containing biometric data**	X	C & D	Video containing recognizable faces, software does not have facial recognition capabilities.
- **Fingerprints**	X	C & D	Fingerprints
- **Palm prints**	X	C & D	Palm prints
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	C & D	Voice recordings
- **Scars, marks, tattoos**	X	C & D	Scars, marks, and tattoos could be visible in photos and videos.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	C & D	DNA profiles will be submitted to the case file in Spartan.
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & B	
- **User passwords/codes**	X	A & B	
- **IP address**	X	A & B	
- **Date/time of access**	X	A & B	
- **Location**	X	A & B	
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A	PIV card data

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	X	Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	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		X	As necessary and appropriate, ATF personnel will share information stored in Spartan among ATF personnel and offices with direct login to system, and permissions will be role based and controlled by the system administrators. ATF members may request access to material within Spartan; their applications will be reviewed and granted either by providing access to the system or providing the information by email.
DOJ Components	X	X		As necessary and appropriate, ATF users will share Spartan information with other DOJ components by email in accordance with organizational rules and policies. Other DOJ component personnel are not provided access to Spartan.

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.**
Federal entities	X	X		As necessary and appropriate, ATF users will share Spartan information with other federal partners by email in accordance with organizational rules and policies and as approved by the case manager. Other agency component personnel are not provided access to Spartan.
State, local, tribal gov't entities	X	X		As necessary and appropriate, ATF users will share Spartan information with other governmental partners by email in accordance with organizational rules and policies and as approved by the case manager. Other agency component personnel are not provided access to Spartan.
Public	X	X		Members of the public can submit Freedom of Information Act (FOIA) requests for ATF information contained in Spartan released by file transfer from the ATF FOIA site, or post.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		As necessary and appropriate, ATF will share case documents with the parties and court as required by discovery rules or court orders.
Private sector	X	X		As necessary and appropriate, ATF users will share Spartan information with private sector partners by email in accordance with organizational rules and policies and as approved by the case manager. Private sector personnel are not provided access to Spartan.
Foreign governments	X	X		As necessary and appropriate, ATF users will share Spartan information with international governmental partners by email in accordance with organizational rules and policies and as approved by the case manager. Foreign government personnel are not provided access to Spartan.
Foreign entities	X	X		As necessary and appropriate, ATF users will share Spartan information with other international partners by email in accordance with organizational rules and policies and as approved by the case manager. Foreign entity component personnel are not provided access to Spartan.

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.**
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.

ATF provides only statistical, aggregated and anonymized, data to the "Open Data" site (www.data.gov). All data that resides in Spartan is processed and disseminated in accordance with legal requirements, federal regulations, and Department policy.

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.

As required by law, ATF provides data subjects with appropriate notice of information collection under the Privacy Act, 5 U.S.C. § 552a(e)(3), e.g., when individuals submit applications for employment or otherwise submit information within the scope of section (e)(3). However, due to the nature of an investigation, individuals connected to that investigation (i.e., suspects) often do not have the opportunity to review a privacy notice.

The following SORNs provide generalized notice to the public:

JUSTICE/ATF-003, "Criminal Investigation Report System," 68 FR 3551, 553 (1-24-03), 82 FR 24147 (5-25-2017); Exemptions Claimed Pursuant to 5 U.S.C. 552a(j)(2). See 28 C.F.R. § 16.106.

JUSTICE/ATF-008, "Regulatory Enforcement Record System," 82 FR 44659 (9-25-2017); Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.106.

JUSTICE/ DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 132 (7-14-2021). Exemptions Claimed Pursuant to 5 U.S.C. 552a (k)(1) and (k)(2), see 86 FR 61687.

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.

Individuals involved in investigations and litigation may receive notification in accordance with federal criminal and civil procedure and court rules; however, for compulsory data-gathering mechanisms, individuals do not have the opportunity to decline to provide the requested data and documents. All information collected is part of existing or requested case data, as captured, or requested through voluntary requests, subpoenas, discovery requests, applications for licenses or permits, search warrants, civil investigative demands. Certain information may be provided voluntarily by the data subject. Notice is not typically provided to individuals for information collected from public sources, because that information is publicly available.

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.

ATF follows Department procedures regarding requests for access to, or amendment of, records pertaining to an individual, including those maintained within a system of records in accordance with the Privacy Act. See https://www.justice.gov/opcl/doj-privacy-act-requests. Privacy Act requests for access to records are processed under both the Privacy Act and the Freedom of Information Act (FOIA), 5 U.S.C. § 552. All such requests are submitted to ATF's Information and Privacy Governance Division for processing and response.

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):** Granted: January 26, 2021 Expires: January 26, 2024 Extension: **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:**
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Spartan has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system operates within the boundary of ATF's primary infrastructure environment, ATF General Support System (GSS), where it is subject to full system monitoring and auditing in accordance with ATF and Department guidelines. All system documentation supporting these activities are maintained within the Department's system of record, Cyber Security Assessment & Management CSAM[13] tool.
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:** Spartan audits at multiple layers, including the network and application processing levels. All logs are generally reviewed on a weekly basis by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, SPLUNK. All logs are forwarded to the DOJ Security Operations Center (JSOC) for automated analysis and review.
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.** All contractors granted access to Spartan are required to sign the DOJ General and Privileged Rules of Behavior, as determined by their role. All associated IT-related contracts within ATF are required to comply with the policies and guidelines defined and documented within the Department of Justice Procurement Guidance Document 15-03, Security of Information and Information Systems, and the DOJ-02 Contractor Privacy Requirements Contract Clause.
X	**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:** All Spartan users are subject to organizational and Department annual computer security awareness and privacy specific training that includes sign off and acknowledgment of the DOJ General and Privileged Rules of Behavior. In addition, all ATF users are required to undergo formal onboarding training that includes Spartan specific training.

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?

[13] DOJ's Cyber Security Assessment and Management (CSAM) tool, provides federal agencies, and IT security managers with a web-based secure network capability to assess, document, manage, and report on the status of IT security risk assessments and implementation of Federal and NIST standards and policies. CSAM provides a centralized and automated system for the management of Plan of Action and Milestones to include creating, tracking, and closing of IT systems.

All Spartan users are required to undergo training and sign formal Rules of Behavior prior to being granted access to data within Spartan. All users are required to use multi-factor authentication or unique usernames and passwords to access their Spartan accounts. Spartan uses ATF's General Support System's (GSS) active directory services to support a single sign-on solution for all Spartan accounts.

All data is encrypted at rest and during transmission outside ATF's secure boundary. Data access is restrictive; users can access only data which they own or are authorized access. Data sharing follows controlled protocol that allows restriction by authorized personnel.

With approval from authorized persons, access to case data is also controlled with the use of access control lists (ACL). An ACL is a list of permissions associated with a system or resource. An ACL specifies which users are granted access and to resource data, as well as what level of permission they are allowed. Users may be granted all rights or limited to read only.

Access and audit logs are maintained within the system and are reviewed by administrators on an ad hoc basis for unauthorized access and other security and performance related concerns.

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.)

Individual users are responsible for ensuring that records processed or disseminated through Spartan are appropriately retained or destroyed. Requirements governing retention and disposition of ATF documents and information are documented within ATF Order 1340.7 Records Control Schedule and are consistent with National Archives and Records Administration regulations and rules.

Data will be retained in the system until the materials are no longer need to be stored on the system, typically after an investigation or inspection has closed and the information is not needed for other cases or investigations, and in line with the NARA record retention schedules 1-23.

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/ATF-003, "Criminal Investigation Report System," 68 FR 3551, 553 (1-24-03), 82 FR 24147 (5-25-2017); Exemptions Claimed Pursuant to 5 U.S.C. 552a(j)(2). See 28 C.F.R. § 16.106.

JUSTICE/ATF-008, "Regulatory Enforcement Record System," 82 FR 44659 (9-25-2017); Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.106.

JUSTICE/ DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 132 (7-14-2021). Exemptions Claimed Pursuant to 5 U.S.C. 552a (k)(1) and (k)(2), see 86 FR 61687.

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.***

Spartan functions as an internal document management library. The privacy risks associated with information collected within Spartan relate to the loss of confidentiality and integrity of the data.

Access by unauthorized entities to sensitive data, including personal information collected for internal personnel management use, investigation, or litigation potentially could lead to compromised, destruction or corruption of that data, exposure of sensitive court records and personal data, and/or disruption to an ongoing investigation or litigation.

To mitigate these risks, only authorized ATF users can access Spartan and individual document access is further limited by access control lists which are implemented and maintained by each data owner. Additionally, ATF uses a number of proven protection methods, including secure communications through DOJ's Justice Unified Network (JUTNET), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques to ensure data is protected in accordance with DOJ IT security standards and applicable U.S. Government standards.

ATF adheres to the DOJ Incident Response Plan for recognizing and responding to unauthorized security-relevant changes to the information system through coordination with the DOJ Justice Security Operations Center (JSOC). ATF relies on the DOJ JSOC for monitoring the network and ATF assets, providing system and data integrity. The ATF Computer Security Incident Response Team (CSIRT) tracks cybersecurity incidents using the DOJ JSOC Incident Management System (JIMS). Traffic at ATF HQ is also monitored by Vectra threat detection software. ATF protects the router and firewall configurations on the Global Enterprise Network Intelligence System with JUTNet protects the integrity of transmitted information by encryption.

The AWS GovCloud is FedRAMP certified and is responsible for ensuring that products meet the standard in NIST 800-53[14], this document provides guidelines for security functionality and assurance to ensure that information technology component products and the information systems built from those products are using sound system and security engineering principles are sufficiently trustworthy.

All application sessions are encrypted using Hypertext Transfer Protocol Secure (HTTPS). Hypertext Transfer Protocol Secure is an encryption protocol that uses a combination of the Hypertext Transfer Protocol (HTTP) with the Transport Layer Security (TLS) protocol which protects the transmitted data from infiltration or interception.

The types of information collected within Spartan vary greatly based on the data owner's needs and investigation requirements. To mitigate the risk of overcollection, information gathered is limited to what is necessary for each specific matter. ATF complies with applicable record retention schedules and guidance, to prevent the storage of records within Spartan for longer than is necessary. ATF provides user training, and annual privacy training to users of Spartan to mitigate the risk of overcollection.

Spartan does contain SSNs as proof of identification for individuals involved with law enforcement investigations and regulatory requirements. To mitigate the risk posed by the processing of SSNs, access to documents containing SSNs are also secured using data encrypted at rest and during transmission outside ATF's secure boundary.

Spartan does contain social media information that is relevant to specific ATF requirements related various investigations. ATF collects social media information only when it is required, within the parameters of the ATF social media standard operating procedures, and consistent with Privacy Act § 552a(e)(7), concerning records describing how an individual exercises First Amendment rights.

[14] NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations" can be found at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final