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

Privacy Impact Assessment
for the
Confidential Informant Master Registry & Reporting System (CIMRRS)

Issued by:
Adam Siple, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: July 5, 2022

(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.)

The Confidential Informant Master Registry and Report System (CIMRRS) serves as The Bureau of Alcohol, Tobacco, Firearms, and Explosives' (ATF) official system of record and repository for all information related to confidential informants and retains several types of personal identifiable information (PII), from name and basic contact details to criminal history information and expenditures paid to informants. CIMRRS is used to create, track, and record confidential informant (CI) information in support of ATF's law enforcement mission.

The ATF Enforcement Support Branch is located within the Special Operations Division and supports field personnel in managing the Confidential Informant Program and its associated registry. CIMRRS is a role-based system allowing access to those authorized ATF users involved in field operations and certain state or local Task Force Officers (TFOs) utilizing informants as part of ATF criminal investigations. ATF may share CI information with ATF-partnering law enforcement agencies only through the partner agencies' assigned TFOs. Other law enforcement agencies will, on occasion, provide Personally Identifiable Information (PII) to ATF for the purpose of deconfliction. If the deconfliction request is regarding a CI, ATF will use CIMRRS to confirm or deny the individual is a past or present ATF CI. CI information may also be shared with members of the United States Attorney's Offices or a state or local prosecutor's office as part of the judicial process. However, members of the United States Attorney's Office (USAO) or state or local prosecutor's office do not have direct access to CIMRRS; requests for CI information must be made to the respective ATF office out of which the CI and their assigned handler are based (i.e., special agent or TFO). The sharing of information, as a result of a request, must be approved by the Special Agent in Charge (SAC) in conjunction with ATF field division counsel

ATF prepared a Privacy Impact Assessment for CIMRRS because ATF collects information in identifiable form about individual members of the public serving as CIs. ATF defines CIs as "person(s) who assist enforcement efforts, providing information and/or lawful services related to criminal and other unlawful activity to ATF that otherwise might not be available," to support investigations. ATF could not effectively achieve its mission without the assistance of CIs. CIMRRS does not contain information on associates or other persons involved in investigations with which the CIs are assisting.

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.

CIMRRS enables ATF to securely maintain CI-related information, including all payments to CIs, length of time that CIs have been active, legal status of foreign national CIs, and special categories of CIs, such as Federal Firearms Licensees and CIs utilized internationally. It also documents authorizations for CIs to perform activities that would otherwise be illegal.[1] This system is only, however, to maintain the data used to decide if a CI can work as a CI, and the management of such CI (e.g., payment, address, lodging). Information related to alleged crimes that CIs report or witness is held in a separate system. Information concerning CIs will not be released to any other agency or organization, unless compelled by warrant, or court order; at which time disclosure of information from a CI record would not be scanned, copied, emailed or released in any transferable media (digital files or printed). The federal, state or tribal legal representative (Assistant U.S. Attorney (AUSA) or state or local prosecutor) would come to the ATF office for a review of the CI record. In cases where the obligation to disclose information is under federal or state law or court order, concurrence from the SAC and Division Counsel is required and will be documented in a memorandum and retained in the record. Other law enforcement agencies will, on occasion, provide PII to ATF for the purpose of deconfliction. If the deconfliction request is regarding a potential CI, ATF will utilize CIMRRS to confirm or deny the individual is a past or present ATF CI.

The CIMRRS user community is comprised of ATF special agents and TFOs throughout ATF field divisions and field offices that serve as CI handlers. ATF Group Supervisors, Resident Agents in Charge, SACs, and Assistant Special Agents in Charge of field offices or divisions use CIMRRS to document the identity of each individual prospective CI and determine if they are suitable and whether information to be provided by the prospective CI is of value to ATF. Field Divisions have multiple CI coordinators that utilize CIMRRS to assist in management and oversight of CI information and compliance with CI policy.

The CIMRRS Inspection user role is utilized (in a limited capacity) by ATF's Office of Professional Responsibility and Security Operations as part of the internal audit process. ATF's CI Project Manager and Project Officer have administrative rights to manage user profiles, address organizational matters, and support all ATF field divisions. All auditable actions taken by system administrators are captured in audit logs within Splunk, which are reviewed on a weekly basis by a cyber security member.

CI records are backed up on the AWS GovCloud, and the records are to be destroyed 10 years after the CI has ceased working for ATF either by removal for cause, or cancellation or withdrawal of the CI. CIMRRS records are covered by the ATF Records Control Schedule O 1340.7, items 3253 and 3255, which has been approved by National Archives and Records Administration (NARA). The FedRAMP certification package for AWS GovCloud: F1603047866 was approved on June 21, 2016, and AWS GovCloud is certified for FedRAMP impact level High for providing Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

---

[1] ATF uses CIs to assist in investigating criminal activity, developing CIs to the point where the individuals will regularly contribute information and, if authorized, perform activity that would otherwise be illegal without such authorization. Since use of a CI is a sensitive matter and requires the association of special agents and task force officers (TFOs) with individuals whose motivations may be suspect or ultimately challenged by courts, this investigative technique shall be carefully controlled and closely monitored. CIMRRS assists ATF in the oversight and management of CIs by providing a repository to track CI activity, including documenting payments and other benefits that may be provided to a CI; documenting authorized illegal activity; calculating the number of days a CI is active; prompting completion of and documenting mandatory semiannual suitability reviews and long-term suitability reviews; recording derogatory information received regarding the CI; documenting when a CI is deactivated or removed for cause.

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
X	Statute	• 28 U.S.C. § 599A. Bureau of Alcohol, Tobacco, Firearms, and Explosives • 28 CFR Subpart W - Bureau of Alcohol, Tobacco, Firearms, and Explosives
	Executive Order	
	Federal Regulation	
X	Agreement, memorandum of understanding, or other documented arrangement	• The Attorney General's Guidelines Regarding the Use of Confidential Informants, (May 30, 2002). • Attorney General Order No. 3363-2013 (February 12, 2013)
X	Other (summarize and provide copy of relevant portion)	• ATF Order 3252.1B, Use of Confidential Informants

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, C & D	**DOJ/Component Employees, Contractors, Detailees** Full name of CI coordinator/handler **Members of public (citizen, USPERs & Non-USPERs)** First, last, and alias
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	Nationality and race
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	Full or truncated
Tax Identification Number (TIN)			
Driver's license	X	C & D	
Alien registration number	X	C & D	
Passport number	X	C	U.S. passport number
FBI Number, Universal Control Number	X	C & D	The Federal Bureau of Investigation (FBI) assigns a unique identifying number used to index an individual's criminal or civil identity record.
Federal Firearms Licensee (FFL)	X	C	A member of the public who is authorized to engage in the business of dealing, manufacturing, or importing firearms
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C & D	
Personal e-mail address			
Personal phone number	X	C & D	
Foreign address	X	C & D	
Business mailing address			
Business e-mail address			
Business phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	C & D	Cash payments issued to CIs

Applicant information			
Education records	X	C & D	
Military status or other information			
Employment status, name of current employer, duration of current employment, history, or similar information	X	C & D	
Employment performance ratings or other performance information, e.g., performance improvement plan			
Current Employment address, supervisor's name, and contact information	X	C & D	
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Criminal affiliations
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Information related to administrative procedures for management and oversight of CIs	X	A	Name and location (to include field division, field office and phone number) of CI coordinator and CI handler
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			While CIs are often witnesses to crimes, themselves, no information about their relationship to ATF cases will be maintained within CIMRRS.
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C & D	
- **Video containing biometric data**			
- **Fingerprints**	X	C & D	
- **Palm prints**			
- **Iris image**			

- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C & D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	ATF system user ID TFOs can include members of state and local law enforcement that have a CI or are signing up a CI and have access to CIMRRS. Not all ATF TFOs have access to CIMRRS. Access is based on each individual's need-to-know.
- **User passwords/codes**	X	A	
- **IP address**		A	IP address at time of system access
- **Date/time of access**	X	A	Date/time of system access
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			Other relevant information may be provided in the free-form field provided for this collection, which may contain PII about individuals related to, or associated with, a CI in this system that is not covered under one of the above categories. ATF will not collect any information from the free text field that is not relevant to its operations and will treat all information collected with the same heightened standard of care.

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	

Phone		Email			
Other (specify): CI personal information is entered into the following forms by the ATF special agent or TFO who will serve as CI handler. ATF Form 3252.2 title: Informant Agreement ATF Form 3252.4 title: Initial Suitability Request ATF Form 3252.5 title: Reactivation Suitability Request					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online, electronic monitoring and notification	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Indices checks, (which refer to the national index of individuals criminal histories) are conducted and criminal history information is obtained from the FBI National Crime Information Center, U.S. Department of Homeland Security's TECS system, the ATF Federal Licensing System[2], and the National Law Enforcement Telecommunications System (NLETS[3]).					

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**

[2] FFL/FEL (Federal Firearms License/Federal Explosives License) are licenses issued by the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) that enables individuals at a company to engage in business pertaining to the manufacture, importation, and interstate/intrastate sales of firearms, ammunition, and explosives.

[3] The National Law Enforcement Telecommunications System (NLETS) is a secure information sharing system that local, state and federal law enforcement agencies use to communicate and share data.

				with the purposes of the collection.
Within the Component	X		X	Access is granted based on job assignment; users are assigned a role in CIMRRS based on the need for either application level (front end) and/or device level (back end) access.
DOJ Components	X			Any disclosure of information from a CI record to an entity outside ATF must be documented in a memorandum and retained in the record. When a USAO or state or local prosecuting office requests information from a CI record, the AUSA or state or local prosecutor may come to the ATF office for a review of the CI record. No CI records are to be scanned, copied, emailed, or released to the AUSA or state or local prosecutors for discovery or other purposes except as referenced above where DOJ is obligated to disclose it by law or court order. In cases where the obligation to disclose information is under state law or court order, concurrence from the SAC and Division Counsel is required.
Federal entities				
State, local, tribal gov't entities	X			Any disclosure of information from a CI record to an entity outside ATF must be documented in a memorandum and retained in the record. When a USAO or state or local prosecuting office requests information from a CI record, the AUSA or state or local prosecutor may come to the ATF office for a review of the CI record. No CI records are to be scanned, copied, emailed or released to the AUSA or state or local prosecutors for discovery or other purposes except as referenced above where DOJ is obligated to disclose it by law or court order. In cases where the obligation to disclose information is under state law or court order,

				concurrence from the SAC and Division Counsel is required.
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.

Any data that resides in CIMRRS is processed and disseminated in accordance with legal requirements, federal regulations, and Department policy. ATF provides only statistics and case filings to the "Open Data" site (www.data.gov); due to the highly sensitive nature of the data contained in CIMRRS and the likelihood of harm to the individuals named, and potentially their associates and family members, if their data was made public, it would not be released publicly.

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.

The following ATF SORNs provide generalized notice to the public:

JUSTICE/DOJ–002 Department of Justice Information Technology, Information System, and Network Activity and Access Records, 64 FR 73585 (12-30-1999); 66 FR 8425 (1-31-2001); 82 FR 24147 (5-25-2017); 86 FR 37188 (7-14-2021).

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.

In addition, a Privacy Act (e)(3) notice is provided on ATF Form 3252.2 title: Informant Agreement; ATF Form 3252.4 title: Initial Suitability Request; ATF Form 3252.5 title: Reactivation Suitability Request.

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 must consent to participate as a CI and provide their personal information. Thereafter, the personal information that the prospective CI provides is used to verify the identity of the individual and their suitability to work as a CI (a background assessment is conducted). If the individual does not consent to providing their personal information, the process to determine their suitability and register them as an active CI will be cancelled, and they will not be used as a CI.

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: Nov 15, 2019 Expires: Nov 15, 2022 **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:** System monitoring, testing and evaluations are completed whenever there is a major change to the system, during annual assessments, and/or when system assessments are required for

	ATO renewal. Requests for changes to CIMRRS are reviewed by a change advisory board before being applied. The core controls are assessed annually, and includes the controls related to the application and though generally inherited from the infrastructure, policy, or parent system. All system documentation supporting these activities are maintained within the Department's Cyber Security Assessment & Management 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:** All CIMRRS audit events are currently being captured in DOJ Splunk[4], including the login events for successful and unsuccessful logon attempts. The login event audit logs currently reside in DOJ's Active Directory Federated Services, which CIMRRS uses for single sign-on authorization service with 2-factor authentication for network access combined with an access control list to restrict access to the CIMRRS application and data. The Splunk dashboard contains all other auditable events, as defined in the DOJ Cybersecurity Services Unclassified Control Matrix and a documented weekly review is conducted. On a weekly basis, the CIMRRS Designated Security Officer (DSO) and/or Local System Administrator (LSA) review the CIMRRS dashboard. The DSO and/or LSA notifies the Splunk manager of any findings or non-findings to log in the Splunk dashboard notes for the week (e.g., failed attempts to access, system errors). A helpdesk ticket is created to investigate any system issues identified on the logs. The helpdesk would work issues that are affecting the back-end of the system software and would not have access to the system data; rather, they would investigate system failures and notify authorized system administrators of potential issues.
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.** Any contractors granted access to CIMRRS are accessing the back-end of the system without access to the data contained and are required to sign the DOJ General and Privileged Rules of Behavior. 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. System owners acknowledge that FAR[5] language is included in the contracts as it would pertain to privacy and system use and the Acquisition Policy Notice 2021-07A.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel**

[4] Splunk captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.
[5] FAR refers to Federal Acquisition Regulation, the government uses federal contracts (FAR-Based Contracts) as a procurement mechanism to purchase property or services for its direct benefit or use. These contracts are governed by a strict set of terms and conditions, including clauses from the FAR and agency specific FAR supplements.

	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 CIMRRS 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 with access to CIMRRS are required to undergo formal onboarding training that includes CIMRRS-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?

ATF secures information in the system by a variety of means, including the following:

Physical access to the ATF site is controlled and monitored by security personnel who check each individual entering the building for their employee or visitor badge.

Transport layer security (TLS) connections and multifactor authentication are used to provide authentication, privacy, and data integrity by encrypting data in transit. ATF provides confidentiality and integrity protection of information at rest by using the Symantec Endpoint Encryption Client 'Whole DISK' encryption to automatically encrypt and decrypt the workstations and laptop computer hard disks, further encryption is provided on the AWS GovCloud instance using server-side encryption utilizing AES-256 encryption. Whole disk encryption encrypts the entire disk including swap files, system files, and hibernation files. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, and only an authorized user can access its contents. Decryption does not occur until the password or passkey is entered. When a user boots into their computer, it will ask them for their password or passkey, which will decrypt everything.

ATF keeps application, network, server, and database activity logs. Audit logs are transferred to Splunk and regularly reviewed for errors and abnormalities.

CIMRRS automatically disables accounts when the user has not logged into the system during the prior 90 days. If this occurs, a user must physically request (via email) to have the account reinstated. User accounts are reinstated only after the CI PM or Project Officer validates the need. The CI PM or Project Officer also disable accounts when notified of a user's separation from ATF or change in position where access is no longer a valid need. These notifications are automatically generated by ATF's ServiceNow, the individual, their first-line supervisor, or the Division CI coordinator.

Access controls and application of the principle of least privilege Role Based Access Control limit access to data based on the user role assigned, giving users access only to the data that is required to do their job. There are 9 types of users with in CIMRRS, which creates a wide array of options for limiting data access.

Information that is alleged to be erroneous or inaccurate by a user who does not have write access is reviewed by the CI PM or Project Officer serving as the HQ Administrator. Corrections that are deemed necessary will be corrected by the HQ Admin or other appropriate user with write access.

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.)

Records are to be destroyed 10 years after the deactivation, removal for cause, or cancellation/withdrawal of each individual CI. CIMRRS is covered by ATF Records Control Schedule O 1340.7, items 3253 and 3255, and operates consistently with National Archives and Records Administration guidance.

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–002 Department of Justice Information Technology, Information System, and Network Activity and Access Records, 64 FR 73585 (12-30-1999); 66 FR 8425 (1-31-2001); 82 FR 24147 (5-25-2017); 86 FR 37188 (7-14-2021).

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.

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.***

ATF uses CIMRRS as an internal management registry for CIs. The privacy risks associated with information collected within CIMRRS primarily relate to the loss of confidentiality, and integrity of the data. When data being protected contains CI information that could be used to identify them, a grave threat is created if the information is not maintained securely. Unauthorized access to, or misuse of sensitive data, including personal information collected for internal personnel management use, investigation, or litigation could potentially lead to death of CIs and their family and associates, destruction, or corruption of data, compromised identities, exposure of sensitive court records and personal data, or disruption to an ongoing investigation or litigation.

To mitigate the risk of unauthorized access to or disclosure of the information, only authorized ATF users can access CIMRRS. Access is controlled by maintaining strict access control lists and enforcing multi-factor logon authentication to ATF devices and network. Users logon with valid Personal Identity Verification (PIV) cards[6] and a Personal Identification Number (PIN). Users are limited by what information they can access by their assigned application role, there are nine different user roles with access and data permissions customized for each providing a layered approach to user management and access control.

Data is protected at rest and in transit with encryption provided by TLS protocol, and full disk encryption. TLS works because it first validates that the user is who they say they are, using their PIV and PIN, and that they have access to the server; this is referred to as the TLS handshake. During a TLS handshake, both user and server send each other random data, which they use to make calculations separately and then derive the same "session keys." These "session keys" these will be used for encryption for the rest of the session. Once a handshake has taken place, and keys have been derived, both the user and the server will have the key, which enables the server to decrypt data from the client using the same key. Data sent between the user and server will be encrypted. Sessions are completed by the user terminating or closing out of the application or by timing out.

Data at rest is protected by using the Symantec Endpoint Encryption Client encryption to automatically encrypt/decrypt the workstations and laptop devices, further encryption is provided on the AWS GovCloud instance using server-side encryption utilizing AES-256 encryption. Whole disk encryption encrypts (converting the readable text into unreadable text or code) the entire disk including swap files, system files, and hibernation files. The encrypted state of the drive remains unchanged, until an authorized user can access its contents using a password or passkey to decrypt the disk.

TLS, whole disk encryption, and multifactor authentication are used to provide authentication, privacy, and data integrity, together, they allow the protocol to authenticate the other party in a

[6] Personal Identity verification (PIV) card are used to validate the identification of the card holder. There are four PKI certificates and they are stored in an area on the credential called the PIV container. The PIV container is in the circuit chip visible on the front of the credential. The four certificates are: Digital signature, Encryption, PIV Authentication, Card Authentication

connection, check the integrity of data and provide encrypted protection.

CIMRRS does contain SSNs which serve as a unique identifiers (UIs) for conducting the background investigation on the CIs. CIMRRS generates an ATF UI when the CI record is created. From that point forward, the ATF UI is used on any documents generated by CIMRRS to identify the CI. Documents generated by the background investigation that contain the SSN are controlled through access control lists and user permissions. Documents containing SSNs are also secured using encryption.

Additionally, ATF uses a number of network 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 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 tracks cybersecurity incidents using the DOJ JSOC Incident Management System. 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 CIMRRS application is hosted in a cloud environment which uses a mixture of on-premise and Federal Risk and Authorization Management Program (FEDRAMP) compliant government cloud hosting services. The infrastructure is aligned with National Institute of Standards and Technology (NIST) security standards. NIST data security standards include NIST 800-53, which offers security controls and privacy controls in the areas of application security, mobile, and cloud computing, and supply chain security, NIST 800-53/FI, which establishes standards to implement FISMA (United States legislation that defines a framework of guidelines and security standards to protect government information and operations), NIST 800-30, which provides guidelines for conducting risk assessments, NIST 800-171, pertaining to the physical security of data centers, and ISO 27001 (international standard for information security. It sets the specifications for an information security management system).

Federal Information Processing Standards 199 requires that federal agencies assess their information systems in each of the categories of confidentiality, integrity, and availability; rating each system as low, moderate, or high impact in each category based on the risks to the system and the impact to the organization if an event jeopardized the information and information systems. The most severe rating from any category becomes the information system's overall security categorization. CIMRRS has been categorized as 'High' due to the nature of the possible catastrophically adverse effect on the individual CIs (and associated persons) the ATF operations, resources, and assets should the CI's information be compromised or exposed. Risks are mitigated using the controlled access and encryption detailed above.

The AWS GovCloud is FEDRAMP-certified and is responsible for ensuring that products meet the current NIST 800-53 standard,[7] which 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.

CIMRRS has no system-to-system communication or connections to any other system where the data contained is shared. However, CIMRRS uses the network single-sign-on which employs multi-factor authentication for access onto the network. Then, access to CIMRRS is protected by an access control list (ACL)[8]. The CIMRRS ACL specifies which users are granted access to the application, as well as what operations they are allowed. Once within the application the case agents control the access to their cases with another ACL. No users who are not in the ACL will be able to access the application.

Any disclosure of information from a CI record to an entity outside ATF must be documented in a memorandum and retained in the record. CI information may be shared with members of the USAO or a State or local prosecutor's office as part of the judicial process. However, members of the USAO or State or local prosecutor's office do not have direct access to CIMRRS; requests for CI information must be made to the respective ATF office out of which the CI and their assigned handler are based (i.e., special agent or TFO). The sharing of information, as a result of a request, must be approved by the SAC in conjunction with ATF field division counsel as described in Section 2.1 above.]

[7] 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.

[8] Access-control list (ACL) is a list of permissions associated with a system resource (object), this can be an application, program or device. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.