Federal Bureau of Investigation

Privacy Impact Assessment
for the
Electronic Departmental Order

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

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

Date approved: [September 20, 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.)

This Privacy Impact Assessment (PIA) is an update to the Electronic Departmental Order (eDO) PIA published in September 2018[1] and the eDO – National Instant Criminal Background Check System (NICS) Appeals PIA published in July 2019.[2] Specifically, this PIA addresses the further expansion of the eDO service to individuals who request inclusion in the Voluntary Appeals File (VAF), which is a file maintained to assist those who are erroneously delayed or denied lawful firearms transfers.

The eDO service is managed by the FBI's Criminal Justice Information Services (CJIS) Division and is a major application/database within the Next Generation Identification (NGI) System, the FBI's biometric and national criminal history repository. The eDO service provides automated, accurate, and timely responses to the public when requests for criminal history records and other benefits are submitted to the FBI. When making DO requests, NICS challenges, and VAF requests, individuals are required to provide biographic information either electronically or manually to ensure the accuracy of their identity. Depending on the benefit sought, individuals may also submit fingerprints for searching in the NGI System. The PIA reflects the additional risk of collecting this personally identifiable information.

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 ana lyses to identify previously unknown areas of concern or patterns.

The eDO service contains Personally Identifiable Information (PII) submitted on DO, NICS, and VAF applications, as well as any supplementary documentation that individuals may choose to send to the CJIS Division. The eDO service within the NGI System provides centralized functions and storage for the automated processing of Departmental Order (DO) requests, NICS challenges, and VAF requests. Unlike the NGI operational environment, the eDO service is not searchable by any of the FBI's partners and access and dissemination of information is strictly controlled, even within the FBI. Information may be submitted electronically via the eDO website or may be submitted hard copy via mail or fax. All hard copies are destroyed after the information is scanned and uploaded into the eDO service.

Departmental Order Requests:

---

[1] See https://www.fbi.gov/file-repository/pia-electronic-departmental-order-edo.pdf/view
[2] See https://www.fbi.gov/file-repository/pia-edo-nics-appeals.pdf/view

On September 24, 1973, the Attorney General issued an Order directing that the FBI publish rules for the dissemination of arrest and conviction records to the subjects of such records upon their request. This order is known as Departmental Order 556-73 and may be found at 28 Code of Federal Regulations (C.F.R.) 16.30-16.34. These regulations identify the procedure to be followed when the subject of a criminal history record requests production of his or her record for review, correction, or updating, or when an individual wants to confirm the absence of a criminal history record. The implementation of this regulatory procedure is the responsibility of the FBI's CJIS Division and is known as the "DO process." The regulations for the DO process predate the enactment of the Privacy Act and were not changed after the implementation of the Act, because the system of records for the DO process was exempted from access requests as provided for by the Act.

In accordance with the DO regulations, the CJIS Division provides a copy of a criminal history record or a finding of no record when an individual submits a written request, satisfactory proof of identity, including fingerprints and biographic data, and a monetary fee. For several decades, the public submitted this information in hard copy format and the CJIS Division responded in the same manner. The eDO service was developed and implemented by the CJIS Division to automate the DO process. Individuals now may choose to submit all required items electronically, all required items manually, or may choose both methods, such as submitting an electronic request and mailing in the fingerprint card.

Individuals submit DO requests electronically via the eDO website[3], which interfaces with the eDO service, or mail/fax hard copy application forms[4] to the CJIS Division. The CJIS Division staff accesses the eDO website processing functions via CJIS UNet, a multi-purpose, unclassified network that supports and provides access to the Internet and various FBI systems, applications, and functions. For the eDO website, the individual must first provide a valid email address to receive a secure link and pin that will permit access to the request form on the website.

The eDO website collects the same information from the public that is collected on the hard copy application form. The eDO website requires name, address, citizenship, date of birth, place of birth, telephone number, email address, and prisoner number (if applicable). Providing either the full or the last four digits of the Social Security Number is optional. The individual must acknowledge the applicable Privacy Act statement before entering the required biographic data on the eDO website. The same Privacy Act statement appears on the hard copy application form.

Individuals submitting DO requests must also provide ten-print fingerprints to be searched in the NGI System to determine the existence of criminal history records and to ensure positive identification. The individual may mail/fax a hard copy fingerprint card to the CJIS Division or provide fingerprints to an authorized entity[5] with an approved electronic connection for transmission to the NGI System. The eDO service generates a unique identifier for each fingerprint transaction sent to search the NGI System. Once the fingerprints have been successfully submitted to the NGI System, the NGI transactional information is available to view from the eDO transaction.

If a criminal history record is located, it will be returned to the requester via the eDO website. The

---

[3] See https://www.edo.cjis.gov
[4] The DO Request Form, I-783, is available at https://www.fbi.gov/services/cjis/identity-history-summary-checks
[5] Governmental and other entities may collect and electronically submit fingerprints to the NGI System if they demonstrate strict adherence to legal, technical, and security requirements promulgated by the CJIS Division.

individual will receive a hard copy response if hard copy fingerprints were submitted or if the individual requested the hard copy option on the eDO website. Criminal history records typically include additional PII, such as the full Social Security Number, race/ethnicity, gender, and alias and maiden names. If no criminal history record is located, the eDO service will generate a letter confirming the absence of criminal history in the NGI System. This letter may be accessed via the eDO website or the CJIS Division will mail a hard copy letter to the requester.

If an individual receives a criminal history record and believes it to be inaccurate or incomplete, the eDO service may also be used to challenge the record. As with the original request, individuals may choose to submit a challenge electronically via the eDO website or mail/fax a hard copy challenge. The Universal Control Number (UCN), which is the unique identity number in the NGI System, or the State Identification Number (SID) from the state criminal history information, must be provided. Pursuant to federal regulations, the CJIS Division works with the individual to confirm the criminal history record, including reaching out to the originator of the records if appropriate. The requester will receive the results of the challenge either electronically via the eDO website or the CJIS Division will mail a hard copy letter.

National Instant Criminal Background Check System Challenges:

The Brady Handgun Violence Prevention Act of 1993 (Brady Act) (18 U.S.C. §922) requires Federal Firearm Licensees[6] (FFLs) to conduct background checks on individuals attempting to purchase a firearm. The Brady Act also created the NICS[7], for FFLs to contact to determine whether the receipt of a firearm by a prospective purchaser would violate state or federal law. Should an individual be prohibited from purchasing the firearm, the Brady Act allows the individual to inquire about the reason for the denial and to challenge the denial status of the firearm purchase transaction. Should an individual believe the denial of a firearm transfer was in error, 28 C.F.R. 25.10 allows the individual to challenge the accuracy of the record upon which the denial was based and to challenge the decision.

The Fix NICS Act of 2017 (34 U.S.C. §40901) requires the FBI to take no longer than 60 days to complete the firearm challenge process. To comply with the 60-day requirement, the CJIS Division processes NICS challenges within the eDO service. The eDO service interfaces with the NICS and Web services are available between the eDO service and the NICS to retrieve status, creation, attachments, cancellation, and closing of firearm challenges.

An individual initially may request the reason the firearm transfer was denied and the CJIS Division must respond to this request within five days. For this inquiry, the individual completes a request for reason for denial application on the eDO website or sends a request by mail/fax with name, NICS Transaction Number (NTN) or State Transaction Number (STN)[8], and a home address. The individual may optionally provide date of birth, maiden name, phone number, email address, the state of firearm purchase, and Social Security Number (full or last four digits) to help identify the correct record

[6] Persons who engage in the business of dealing in firearms and are licensed by the Bureau of Alcohol, Tobacco, Firearms and Explosives.
[7] See https://www.fbi.gov/file-repository/pia-nics.pdf/view
[8] The NTN and STN are unique numbers assigned by the FBI or State point-of-contact for firearm-related background check inquiries.

information that may be relevant to the request. The individual must acknowledge the applicable Privacy Act statement before entering the required biographic data on the eDO website.

The information entered by the individual is sent to the eDO service which queries the NICS system to ensure the individual's stated NTN/STN is valid. If valid, the eDO service uses the NTN/STN to query the NICS system to determine the reason for the NICS denial of the firearm purchase. If the NTN/STN is valid and a federal or state prohibited category is returned, the requester may obtain the reason for the denial by accessing the eDO website or, upon request, the CJIS Division will send a hard copy letter to the requester. As with the DO process, the individual is provided with a secure link and pin to access the eDO website. A copy of the request and the response are sent to NICS and retained or purged per NICS retention policies. The letters are maintained in the eDO service for a period of 88 days after being sent to the individual, and then deleted.

If the individual initiates a NICS challenge after learning the reason for the denial, he or she must submit an application on the eDO website or mail/fax a written challenge to the CJIS Division. The same PII is collected as with the original firearms inquiry, along with optional fingerprints. The individual may mail a hard copy fingerprint card to the CJIS Division or provide fingerprints to an authorized entity with an approved electronic connection for transmission to the NGI System. Once the challenge is received, the eDO service queries the NICS system for the reason for the firearm denial and CJIS personnel perform additional research in authorized CJIS systems , such as NGI and the National Crime Information Center (NCIC), to determine the existence of disqualifying information. If fingerprints are submitted, the eDO service transmits the fingerprints to the NGI System to search for relevant criminal history record information.

The research and system searches performed by CJIS personnel determine if the individual's criminal history or other relevant data prohibits the purchase of a firearm. These research findings and system responses are returned to the eDO service. Once CJIS personnel determine whether to confirm or overturn the denial, a response is generated and made available electronically on the eDO website and/or by a mailed hard copy letter. If the individual has no criminal history record, the response letter will only contain the individual's name and address and will confirm or overturn the denial. If the individual's conviction was overturned, the eDO service generates a response letter, and provides a certificate of this fact to the individual. Individuals who have submitted fingerprints and who have a criminal history record will receive the criminal history record, including all available arrest and disposition information.

All PII and associated documentation are purged within 88 days from the eDO service and only the NTN/STN and eDO transaction numbers are retained for statistical and administrative purposes. Likewise, the NGI System does not maintain the fingerprints or any associated PII related to the NICS challenge fingerprint search. The eDO service sends the original request to the NICS system for retention, along with all criminal history information, research, notes, and official responses.

Voluntary Appeal File Requests:

The VAF was designed for firearm purchasers who believe they are legally permitted to purchase firearms but who have been denied or frequently experience delays. As previously discussed, the Brady Act requires FFLs to conduct background checks on individuals attempting to purchase a firearm. Because it is a name-based system per statute, the NICS may cause individuals to experience

erroneous denials or continuous delays regarding their eligibility to purchase firearms if their identifying information (e.g., name, date of birth) matches that of a prohibited individual. The VAC is designed to help individuals clear up these errors.

For firearms purchases that are permitted to proceed, the NICS must destroy all identifying information within 24 hours of the FFL being notified of the transaction's proceed status. For delays and denials, the NICS generally must destroy all relevant information if the potential purchaser successfully challenges the decision. For these reasons, the creation of the VAF was necessary to permit the NICS to maintain personal information regarding potential firearms purchasers. Established under 28 C.F.R. 25.10(g), the VAF allows for the retention of identifying information which will prevent future denials or extended delays for the potential firearm purchaser.

As with the DO requests and NICS challenges, the eDO service provides centralized functions and storage of information necessary for the automated processing of VAF requests. Individuals must submit required biographic information and ten-print fingerprints, either on hard copy forms or electronically via the eDO website. The individual may mail/fax a hard copy fingerprint card to the CJIS Division or provide fingerprints to an entity with an approved electronic connection for transmission to the NGI System.

As with the other services, VAF applicants must first provide a valid email address to receive a secure link and pin from the eDO website, which will be used to submit the VAF application and to receive future updates and communications regarding the request. The individual must acknowledge the VAF Privacy Act statement before entering the required biographic data on the eDO website. The hard copy VAF application form contains the same Privacy Act statement. The mandatory biographic fields are as follows: last name, first name, mailing address, state of residence, country of citizenship, date of birth, place of birth, sex, race, and ethnicity. The electronic VAF application and the hard copy VAF application form require and collect the same information pertaining to the individual.

Once all required information is transferred electronically or uploaded manually into the eDO service, the fingerprints are searched in the NGI System for any relevant criminal history records. The fingerprints are not retained within the NGI System operational environment after the search is completed. The NGI System response will be retained in the eDO service and, for VAF approvals, the NGI System response will also be retained in the NICS. In addition, the eDO service sends system queries to the NICS based on the NTN/STN and biographic information provided on the VAF application. The NICS queries other relevant databases and CJIS systems to determine if any disqualifiers exist to deny the VAF application. The results of these queries are returned to and maintained in the eDO service until a final resolution has been determined.

At the conclusion of the VAF application process, a determination of approved or denied is made based on the results of the fingerprint search and the NICS research. When an application made via the eDO website is denied for entry into the VAF, the individual will receive the denial letter electronically with details regarding the reason for the denial and a copy of the relevant criminal history record, if applicable. When a hard copy VAF application form is denied for entry into the VAF, a letter with the same information and any applicable criminal history will be sent to the mailing address provided by the individual.

If an individual is approved for placement in the VAF, he or she receives a Unique Personal

Identification Number (UPIN) to be utilized for all future attempts to purchase a firearm. The UPIN holder still must undergo a complete background check to buy a firearm; however, the UPIN aids in confirming the potential firearm purchaser's eligibility to obtain the firearm. The individual will receive the UPIN in the same manner as described above: either electronically via the eDO website or by letter to the mailing address provided. The VAF application, any submitted documentation, and the fingerprint card are not returned to the individual.

For both VAF approvals and denials, the eDO service transfers all biographic information, fingerprints, and eDO notes and attachments to the NICS for retention. For both VAF approvals and denials, the eDO service maintains the biographic information, eDO notes and attachments, and fingerprint cards for three years in accordance with its records retention schedule. For VAF approvals, the information also remains in the VAF, managed by the NICS Section, indefinitely or until the individual requests to be removed from the VAF.

Finally, the eDO service contains an eDO Daily Activity Log which serves as an internal worklog for CJIS Division personnel. The information entered in the Daily Activity Log includes quantity and time for categories such as meetings, mandatory training, and analytical support. Notes entered in the Daily Activity Log are typically brief (i.e., short, bulleted information) and provide titles of meetings attended, type of training completed, and additional information about analytical support provided. The eDO Daily Activity Log does not include any PII.

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. § 534; 18 U.S.C. § 922; 34 U.S.C. § 40901
	Executive Order	
X	Federal Regulation	28 C.F.R. 16.30-16.34, 28 C.F.R. 25.10
	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.

Because any person may request a criminal history record search, challenge the denial of a firearms purchase, or request to be placed in the VAF to avoid delay or denial of future firearms purchases, the below chart includes DOJ and federal government personnel, in addition to members of the public, for each category of PII.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	
Date of birth or age	X	A, B, C, D	
Place of birth	X	A, B, C, D	
Gender	X	A, B, C, D	
Race, ethnicity or citizenship	X	A, B, C, D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	Social Security numbers are optional for Departmental Order, and NICS Challenges, however, criminal histories likely will contain SSNs.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name	X	A, B, C, D	
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	
Personal e-mail address	X	A, B, C, D	
Personal phone number	X	A, B, C, D	
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	A, B, C, D	
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			

(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
Certificates			
Legal documents	X	A, B, C, D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	
Juvenile criminal records information	X	A, B, C, D	
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**	X	A, B, C, D	
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**			

(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
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Unique identifying numbers such as NTN, STN, UCN, SID.

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): Information is generally not received via phone; however, the CJIS Division may phone an individual to clarify information or the individual may phone the CJIS Division to request information.					

Government sources:					
Within the Component		Other DOJ Components		Online	
State, local, tribal		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		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			The eDO service interfaces with the NGI System, NICS, and CJIS UNet to collect and research the relevant PII.
DOJ Components				

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				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			To the individual requesting his/her criminal history record or information related to a NICS challenge or inclusion in the VAF. Information may be sent to an authorized 3rd party, such as an attorney or guardian.

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.

Not applicable.

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.

All personal information provided to the eDO service is provided voluntarily with the individual's notice and consent. For DO requests, individuals voluntarily provide PII to obtain their criminal history records or to confirm the absence of such records. For NICS challenges, individuals voluntarily provide PII to obtain the reason their firearms purchases were denied and to correct or update that information if appropriate. For VAF requests, individuals voluntarily provide PII to allow the FBI to maintain such information to avoid future delays or denials of firearms transfers. In addition, the eDO website provides separate Privacy Act

statements for each benefit sought. The same Privacy Act statements are provided on the hard copy application forms. When individuals submit fingerprints, they receive a separate Privacy Act statement specific to the fingerprint collection and searching. The NGI System's SORN provides general notice of the collection and use of fingerprints and associated biographic information. The most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general notice, as does the previously published PIAs regarding the eDO service.

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.

All information is provided voluntarily by the individual and the individual is informed as to the FBI's uses of the information with specific Privacy Act statements.

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.

Title 28 C.F.R. part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; 28 C.F.R. part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. As discussed earlier in this PIA, 28 C.F.R. §§ 16.30-16.34 establish specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. In addition, the processing of the NICS challenges provides access and amendment regarding system information used to deny firearms transfers. The eDO service was largely created in order to improve public access and amendment to the NGI System and other relevant CJIS Division information.

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):** issuance date: January 9, 2022; expiration date: January 23, 2023. **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: No POAMs related to privacy controls**.**
	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:** The NGI System, including the eDO service, is continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
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:** Host operating system logs are consolidated into the CJIS enterprise system audit consolidation and monitored for irregular activities or compliance failures. The NGI System Security Administrator reviews security-related logs on a weekly basis.
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**.
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:** User Training, specific to this system, is provided to CJIS Division personnel responsible for supporting the eDO service.

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?

User access to information within the NGI System and the eDO service is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. All CJIS Division users of the eDO service are required to have an NGI System account as well as the necessary roles assigned specific to the eDO service. Only CJIS Division staff who are directly responsible for supporting the eDO service have access to the PII, fingerprints, and associated information submitted for the DO requests, NICS challenges, and VAF requests. The information is further protected by role-based controls and access control lists at the group and individual level.

Processes are in place to ensure that only authorized users have access to data protected by privacy law and is verified through audit logs. User activity is audited by system administrators on a weekly and event-driven basis. Auditing of the eDO service occurs from user logs, monitoring application use, and user activity. Auditing functionality identifies what data has changed, who made the changes, and when the changes were made.

The CJIS Division users have been trained to minimize the use, collection, and retention of PII to what is necessary to accomplish their business purpose and mission. Every member of the

CJIS staff has undergone privacy and security training to ensure that information is properly handled. The eDO service is a password protected application, which guards against unauthorized access and disclosure. The use of unique user IDs and strong passwords makes it difficult for a user to gain unapproved access or a heightened level of access. All users are notified through warning banners and by signing the FBI Rules of Behavior that they are subject to periodic, random auditing of what searches they perform, when they perform the searches, and what data was accessed in all FBI information systems. This awareness is useful in discouraging unauthorized searching and to provide awareness of data that has specific handling requirements or sensitivity.

The risk of unauthorized disclosure is further mitigated because the maintenance and dissemination of information must comply with provisions of any applicable law, regulation, or policy, including the Privacy Act. Among other requirements, the Privacy Act obligates the FBI to make reasonable efforts to ensure the information that it disseminates is accurate, complete, timely, and relevant.

The eDO service uses the management, operational, and technical controls within the NGI System infrastructure and operating environment. The eDO service is subject to extensive security protections, access limitations, and quality control standards. All FBI workstations and servers that access eDO information are secured in accordance with FBI security requirements and are verified prior to establishing network connectivity. In addition, all hardware is housed within FBI facilities that have achieved site security accreditation. The NGI System NIST 800-53 security control baseline is at the HIGH impact level of assurance.

The eDO service relies on the security controls provided by the CJIS Shared Enterprise Network (SEN) and FBI Trusted Internet Connectivity (TIC) services. The SEN and TIC include the following network services: virus scanning, packet inspection, denial of service protection, integrity, and confidentiality, where applicable. The eDO service connectivity to the eDO website is securely managed by the SEN and TIC XML gateway devices and the data is encrypted while in motion. The eDO service's Internet–facing web servers are deployed on a set of servers that exist within a private Virtual Local Area Network that is terminated on a firewall to provide an additional layer of logical separation from other hosts within the trusted network. This logical separation forces the traffic from these hosts to be routed through the firewall before being permitted to access other hosts within the trusted network. The eDO service is deployed on an NGI provided Linux operating system baseline that is customized and hardened to accommodate the necessary software. The eDO service leverages NGI's Lightweight Directory Access Protocol services for authentication and authorization for internal users accessing the database.

An Information Systems Security Officer (ISSO) and an Information Systems Security Engineer (ISSE) are responsible for ensuring the day-to-day implementation, continuous monitoring, and maintenance of the security configuration, practices, and procedures for the NGI System and the eDO service. The ISSO/ISSE assists the operational staff and program office to make certain that system security documentation is developed, maintained, reviewed, and updated to reflect changes to the risk posture and privacy impact of the eDO service.

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.)

The National Archives and Records Administration (NARA) has approved the destruction of all electronic documents related to the eDO service (e.g., fingerprint cards, request forms) after three years of processing. The published NARA records schedule is number N1-065-10-16. The hard-copy records are destroyed immediately once electronically scanned and uploaded into the eDO service. Although NICS challenges are processed in the eDO service, any firearms-related challenge information is retained for only 88 days per the Brady Act. The optional fingerprint cards submitted for NICS challenges are deleted immediately and automatically after searching the NGI System. It is important to note that the searching of these fingerprints in the NGI system does not follow the standard search and retention rules of criminal and civil fingerprints in the NGI System; rather the searching of fingerprints submitted for personal benefit is more limited in scope and use.

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:

The NGI SORN is published at 81 Fed. Reg. 27,284 (May 5, 2016): 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg 54, 182 (Oct. 9, 2019).

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.

The CJIS Division collects only the PII necessary to confirm an individual's identity and to complete all necessary research for the DO requests, NICS challenges, and VAF requests. The right to submit these requests and challenges is granted by statutes and regulations, and the CJIS Division must collect information sufficient to ensure accurate and comprehensive responses to the requesters. All information is submitted voluntarily and directly by the individual. The submitted information is used by CJIS Division personnel to process the requests and challenges, including a criminal history record check of the NGI System. Individuals receive specific Privacy Act statements, depending on the benefit sought, for the submission of biographic information and fingerprints. Hard copy records are not retained, and electronic records are maintained only as long as reasonably needed to process the requests and challenges, up to a maximum of 3 years for the DO and VAF requests and up to a maximum of 88 days for the NICS challenges.

The implementation of the eDO service for the DO requests, NICS challenges, and VAF requests greatly improves the accuracy of PII submitted to the CJIS Division and reduces the possibility of lost requests and applications in the mail. By using the eDO website, individuals electronically submit their requests and enter their own relevant information. Having the individual enter his or her own PII reduces data entry errors and placing all communications online avoids risk of U.S. Postal Service delivery. The CJIS Division returns responses to requests and challenges only to the requester or to a person designated by the requester, such as an attorney.

The use of the eDO service for processing requests and challenges greatly reduces the risk of PII breaches. The responses are transmitted electronically via the eDO website and eliminate the possibility of PII and other sensitive information, such as criminal history, being lost in the mail. The use of a unique pin number to access the eDO website safeguards against the possibility of an individual wrongfully accessing another's PII or criminal history. For instances where hard copy responses are requested, the CJIS Division has several stringent quality control measures in place to ensure that the information is returned to the correct person. Should the information be sent to the wrong person, the CJIS Division has a mitigation policy in place in compliance with FBI and DOJ PII breach guidance. If a requester has no criminal history record, the CJIS Division returns a letter that contains minimal PII in order to safeguard against a breach.

Finally, as discussed in Section 6.2, the PII submitted to the eDO service is protected by strict system and personnel security measures. The NGI System provides a secure infrastructure for storage and processing of the information, and access to the eDO service is strictly limited to trained CJIS Division personnel assigned to the specific task of managing eDO requests. Overall, the public has made a significant transition from manual requests to electronic requests via the eDO website. This transition has assisted the CJIS Division with safeguarding the security and privacy of the public's personal information, biometrics, and associated record responses.