Federal Bureau of Investigation

Privacy Impact Assessment
for the
Electronic Departmental Order-NICS Appeals

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

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

Date approved: July 24, 2019

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

EXECUTIVE SUMMARY

The Brady Handgun Violence Prevention Act of 1993 (18 U.S.C. §922) requires Federal Firearm Licensees[1] to conduct background checks on individuals attempting to purchase a firearm. Should an individual be prohibited from purchasing the firearm, the Act also allows the individual to inquire about the reason for the denial and to appeal the denial status of the firearm purchase transaction. The Fix NICS Act of 2017 (34 U.S.C. §40901) further requires the Federal Bureau of Investigation (FBI) to take no longer than 60 days to complete the firearm appeal process.

To comply with the 60 day requirement, the Criminal Justice Information Services (CJIS) Division of the FBI leveraged efficiencies of its electronic Departmental Order (eDO) process, which had previously automated the dissemination of criminal history records to individuals upon their request. As such, this Privacy Impact Assessment addresses the expansion of the eDO process to include appeals of firearms denials. The eDO process for criminal history records is fully described in a separate Privacy Impact Assessment.[2]

Section 1: Description of the Information System

(a) the purpose that the records and/or system are designed to serve;

The Brady Handgun Violence Prevention Act of 1993 required the Attorney General to establish the National Instant Criminal Background Check System (NICS). This system is used to conduct background checks on potential buyers of firearms. The purpose of the background check is to provide a timely determination of a person's eligibility to possess firearms or explosives in accordance with the federal law.

Descriptive data provided by the prospective buyer is searched and verified against the records contained in the FBI's CJIS systems, such as the National Crime Information Center (NCIC), the Next Generation Identification (NGI), and the NICS Indices.[3] Descriptive data includes: name, sex, race, date of birth, state of residence, height, weight, place of birth, Social Security number, or miscellaneous identification numbers such as alien registration and military numbers.

The CJIS systems are searched in order to approve or deny the purchase of a firearm. CJIS denies the transfer of a firearm when the biographic data provided by the prospective buyer matches to federal or state prohibiting criteria. Federal law prohibits any person from possessing or receiving a firearm who:

- Has been convicted of a crime, or is under indictment for a crime, punishable by imprisonment exceeding one year.

---

[1] Persons who engage in the business of dealing in firearms and are licensed by the Bureau of Alcohol, Tobacco, Firearms and Explosives.
[2] *See* https://www.fbi.gov/file-repository/pia-electronic-departmental-order-edo.pdf/view.
[3] The NICS, NCIC, and NGI systems are covered by additional Privacy Impact Assessments.

- Is a fugitive from justice.
- Is an unlawful user of or addicted to any controlled substance.
- Has been adjudicated as a mental defective or committed to a mental institution.
- Is illegally or unlawfully in the United States.
- Has been discharged from the Armed Forces under dishonorable conditions.
- Has renounced U.S. citizenship.
- Is subject to a court order that restrains the person from harassing, stalking, or threatening an intimate partner or child of such intimate partner.
- Has been convicted of a misdemeanor crime of domestic violence.

Should an individual believe his denial of a firearm transfer was in error, 28 CFR 25.10 allows him to challenge the accuracy of the record upon which the denial was based and to appeal the decision.

CJIS has developed the eDO to provide a secure and efficient means to process requests for, and challenges to, criminal history records. An eDO application/database hosted on NGI maintains and manages criminal history record requests and challenges. NGI is the FBI's system that maintains criminal history records and associated fingerprints. An eDO website permits the public to submit requests and challenges and to receive responses electronically.

Due to the passage of the "Fix NICS Act" on March 23, 2018, CJIS must complete appeals of firearms denials within 60 days of the receipt of the documentation to correct, clarify or supplement records of the system. CJIS identified the existing eDO process as a means for also completing firearms appeals in a timely manner.

(b) the way the system operates to achieve the purpose(s);

There are two options an individual may exercise regarding a firearm denial. Phase I is when an individual requests the reason that the firearm transfer was denied. CJIS must respond to this request within 5 days. After learning the reason for the denial, the individual may (but is not required to) initiate Phase II, which appeals the reason for the denial. At that point, CJIS performs the necessary research to determine if the denial should be upheld or overturned.

For Phase I, the individual completes a request for reason for denial application on the eDO website or by mail by providing: name, NICS Transaction Number (NTN) or State Transaction Number (STN)[4], 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 information that may be relevant to the request.

If the application is submitted on the eDO website, the individual is provided with a unique Internet link and pin to access the status of the request. The information entered by the individual is sent to the eDO application which queries the NICS system to ensure the

[4] The NTN and STN numbers are NICS system-assigned unique identifiers for each firearm purchase.

individual's stated NTN/STN is valid. If valid, the eDO application uses the NTN/STN to query the NICS system to determine which one of the prohibited categories (called a PCA Code) was the reason for the NICS denial of the firearm purchase.

The eDO application then generates one of three responses. If the NTN/STN is invalid, a letter explaining the need for a valid NTN/STN is sent to the individual. If the NTN/STN is valid but no PCA Code is associated with the transaction, the firearm transaction was not denied by NICS and a not-denied letter is sent to the individual. If the NTN/STN is valid and a federal or state prohibited category is returned, the reason for the denial based on a NICS prohibitor is placed into a letter and is sent to the individual. The individual will receive email messages when any of these letters are ready for retrieval on the eDO website. If the individual requests, the letters may be sent hard copy via the U. S. Postal Service. As NICS is the system of record for the NTN, a copy of the request and the response are sent to NICS and retained or purged per NICS retention polices. All of the letters are maintained in the eDO database for a period of 88 days after being sent to the requester, and then deleted.

For Phase II, the individual initiates a firearm appeal by submitting an application on the eDO website or with a written request mailed to CJIS. The same personally identifiable information (PII) is sent as in Phase I, along with an optional tenprint fingerprint card. The fingerprint card may either be mailed or attached to the online application. Fingerprint cards and any other supplementary information placed on the eDO website are transferred to the eDO application and all mailed information is scanned and placed into the eDO application. If fingerprints submitted via the eDO website are not of sufficient quality, the individual will be notified to send in a hard copy fingerprint card. Hard copies of fingerprint cards and/or supplementary information are destroyed after being scanned into the eDO database.

Once the appeal is received, the eDO application determines if a challenge for this NTN/STN was conducted within the last 30 days. If so, a letter is sent to the individual explaining a current request for the NTN is pending and a new request for the NTN will not be processed. If a current request is not pending, eDO queries the NICS system, which returns the reason for the firearm denial (just like in Phase I). CJIS personnel then perform research in authorized CJIS systems to determine the existence of disqualifying information and the eDO application queries the fingerprints in NGI to determine if the individual has relevant criminal history record information.

The research and system searches performed by CJIS personnel determine if the individual's criminal history, NCIC records, NICS Indices records, or other relevant data prohibits the individual. These records are returned to eDO, along with the research findings of the CJIS employees. Once CJIS personnel determine whether to confirm or overturn the denial, a response is generated to the individual electronically on the eDO website and/or by hard copy sent via the U. S. Postal Service. If the individual has no criminal history information, the response letter will only contain the individual's name and address and will confirm or overturn the denial. If overturned, eDO generates and sends a response letter, and overturn certificate if applicable, to the individual. Individuals who have submitted fingerprints and who have a criminal history record will also receive that criminal history record, including all available arrest and disposition information.

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

It should be noted that individuals may also appeal the denial of the transfer of explosives, the issuance of firearms permits, or the transfer of firearms pursuant to Nuclear Regulatory Commission authorities (i.e. "non-Brady transactions"). It is possible that these appeals may be initiated via the eDO website and placed into the eDO application/database; however, once CJIS personnel determine that these are not Brady transactions, the appeals will be forwarded to the appropriate entity.

(c) the type of information collected, maintained, used, or disseminated by the system;

The eDO process for firearm appeals will continue to collect the same information from the public that had been collected under the original NICS appeals process. Requesters typically submit name, maiden name, aliases, gender, race/ethnicity, date of birth, home address, telephone number, email address, scars, marks, tattoos, physical characteristics, NTN/STN, state of firearm purchase, and any other relevant information the requester chooses to provide on the eDO website. Optionally, the requestor may provide a full or partial Social Security number and/or fingerprints to retrieve criminal history and to ensure positive identification.

(d) who has access to information in the system;

Only CJIS personnel supporting the eDO application/database and the NICS appeals process have access to the PII, fingerprints, and associated information submitted for the firearm denial appeals.

(e) how information in the system is retrieved by the user;

Individuals submit applications and firearms-related appeals via the eDO website or by mail. If the individual provides an email address, eDO will email a secure link and pin to permit the individual to access the application process on the eDO website. The link and pin must be used within 10 days or it becomes invalid. Once the individual accesses the eDO website, the link and pin continue to be valid throughout the application/appeal process until 90 days after the final response is sent to the individual. The link and pin do not provide access to any personal information; the relevant personal data is entered by the individual during the course of the application/appeal process.

The CJIS 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. All CJIS users of the eDO application/database access eDO with a specialized NGI account, with necessary roles assigned specific to eDO.

(f) how information is transmitted to and from the system; and

The eDO public website (www.edo.cjis.gov) allows requesters to submit appeals to CJIS for NICS denials. Depending on the individual's request and/or appeal, the eDO application will generate the appropriate letters, decisions, and records related to the request and/or appeal that may be accessed by the individual via the website.

CJIS will continue to support the submission of hard copy requests and appeals via the U.S. Postal Service. Requesters 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 a fingerprint card.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects).

The eDO application/database is hosted on the NGI system. It uses the management, operational, and technical controls of the NGI infrastructure and operating environment. The eDO application has approved interfaces with NGI, NICS, and CJIS UNet.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security (Optional)	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify): The information on the ATF Form 4473 is provided to determine whether an individual is prohibited from receiving a firearm. The social security number is optional on the form, and therefore, remains optional in eDO.					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth		Financial info	
Alias	X	Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	

Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

Other information (specify)
NICS Transaction Number (NTN) or State Transaction Number (STN)
State of firearm purchase
The appeals application on the eDO website contains a free text field for the individual to enter any potentially relevant information.

2.2 Indicate sources of the information in the system. (Check all that apply.)

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

Government sources					
Within the Component		Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected

and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The FBI collects only that information which is necessary to confirm an individual's identity and to complete all necessary research for the firearm appeal. The right to appeal a firearm denial is ensured by statute and regulation and the FBI must collect information sufficient to comprehensively review the firearm denial. All information is submitted voluntarily by the individual and the FBI does not collect PII from other sources in order to process a firearm appeal. The submitted information will be used by CJIS personnel to research the reason for the denial, including a criminal history record check of NGI. CJIS will not maintain hard copy records and will only maintain the information electronically in eDO as long as reasonably needed to process the firearm appeal or to resolve another request or concern of the individual, up to a maximum of 88 days.

Notably, the new eDO firearms appeals process should greatly improve the accuracy of PII submitted to the FBI and reduce the possibility of lost requests and applications in the U.S. mail. By using the eDO website, individuals electronically submit firearms appeals and enter all of their own relevant information. Having the requester enter his or her own PII should reduce data entry errors and placing all communications online will avoid the risk of U.S. Postal Service delivery.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): to process NICS appeals pursuant to 18 U.S.C. § 922.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Federal regulations identify the procedure to be followed when an individual requests the reason for a firearm denial and when an individual appeals that denial. In accordance with the regulations, CJIS uses the PII and associated information provided by the requester to confirm identity and to provide a copy of a criminal history record or other reason for firearm denial.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 U.S.C. § 534; 34 U.S.C. § 40901, 18 U.S.C. § 922
	Executive Order	
X	Federal Regulation	28 CFR 25.10(c)-(e)
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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 process (e.g. fingerprints cards, request forms) after three years of processing. Although firearms appeals are processed in eDO, any firearm related appeal information is retained for only 88 days per the Brady Handgun Violence Prevention Act of 1993 (18 U.S.C. § 922). The optional fingerprint cards are deleted immediately and automatically after searching in NGI for criminal history information. Hard-copy information is destroyed immediately once electronically scanned into the eDO application/database. The NARA schedule for eDO will be updated to reflect the firearms-specific retention limitations.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

In accordance with the NICS regulations, CJIS provides the reason for upholding or overturning a

firearm denial, which may include a copy of a criminal history record, when an individual submits a written or electronic appeal and an optional fingerprint card. The automation of the firearms appeals information in eDO greatly improves the security of the personal information submitted by the public and the appeals information returned to members of the public. All FBI users of the eDO application/database are required to have an NGI account as well as the necessary roles assigned specific to eDO. Only CJIS employees who are directly responsible for supporting the NICS appeals will have access to firearms appeals transactions in eDO. The eDO application will provide auditing functionality for NICS appeals to identify what data has changed, who made the changes, and when the changes were made. The CJIS users have been trained to minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. The eDO application/database will be subject to extensive security protections, access limitations, and quality control standards. 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 routine and event-driven basis. Every member of the CJIS staff has undergone privacy and security training to ensure that information is properly handled.

PII Confidentiality Risk Level:

☐ **Low** ☐ **Moderate** ☑ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
n/a	Separation of Duties: eDo users are not able to de-identify or re-identify PII data.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
n/a	User-Based Collaboration and Information Sharing: eDO is used for dissemination of criminal history records and other appeals information to the requester or designee; it will not be disseminated to othe
n/a	Access Control for Mobile Devices: FBI personnel cannot access the eDO application via mobile devices; however the public may retrieve its information from the eDO website using any web-enabled device. The eDO application security boundary ends at the FBI's Demilitarized Zone (DMZ) of the Trusted Internet Connectivity (TIC). The personal mobile devices are outside of the security boundary of eDO but all Internet traffic to and from eDO is encrypted to protect the data until it reaches the individual's mobile device.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access.
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality.

Media controls

X	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled with distribution/handling caveats.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted or stored in a locked container during transport.
X	Media Sanitation: media is sanitized prior to re-use.

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
	Protection of Information at Rest: information stored on a secondary storage device (e.g., hard drive or backup tape) is encrypted. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
(Explain how the privacy risks associated with controls not checked are otherwise mitigated) PII is maintained on the eDO application only during processing and dissemination. The eDO application uses the CJIS Enterprise Storage System (ESS) for primary storage. The ESS is the underlying storage and back-up services for all of CJIS systems. Secondary storage is via data replication to an offsite datacenter using the ESS.	

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X(NICS system)	
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			To the person submitting a firearm denial inquiry or appeal. At the person's request, information may also be sent to an attorney, guardian, or other authorized entity/agency.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

Information in response to a firearm appeal will be disclosed only to the requester or to a person designated by the requester, such as his attorney. Hard copy responses generally are sent via U.S. Postal Service and several quality control measures are in place to ensure that the information is returned to the correct person. When processing the firearms appeals manually, information may be sent to the wrong individual or become lost in the mail. For example, CJIS personnel may correlate an individual's fingerprints with another individual's biographic information or may mistype an address. In many instances, CJIS cannot identify any mistake on its part; however, the requester will report that an appeal response has not been received. For these reasons, CJIS follows stringent quality control measures to limit such incidents and has a mitigation policy in place for when such an incident does occur. If a requester has no criminal history record, CJIS returns a letter that contains minimal PII in order to safeguard against a breach. If CJIS mails a criminal history record that is not received by the requester, CJIS offers credit protection to the individual.

The use of the eDO application for processing firearms appeals will greatly reduce the risk of PII breaches. The responses will be 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 essentially eliminates the possibility of an individual wrongfully accessing another's PII or criminal history.

The eDO application relies on the security controls provided by the CJIS Shared Enterprise network (SEN) and FBI 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 connectivity to the eDO websites will be securely managed by the SEN and TIC XML gateway devices. The data will be encrypted while in motion. The eDO's internet–facing web servers are deployed on a set of servers that exist within a private Virtual Local Area Network (VLAN) that is terminated on a firewall in order to provide an additional layer of logical separation from other hosts within the trusted network. This logical separation forces all of the traffic from these hosts to be routed through the firewall before being permitted to access other hosts within the trusted network.

The eDO application is deployed on an NGI provided Linux operating system baseline that is customized and hardened to accommodate the necessary software. The eDO application leverages NGI's Lightweight Directory Access Protocol (LDAP) services for authentication and authorization for internal users accessing the database. All eDO users are NGI users with modified accounts. All users of the eDO application will be required to have an NGI LDAP account as well as the necessary roles assigned for accessing the eDO application. The groups and roles are tailored to specific functions and tasks. Users cannot perform roles not specified within the assigned groups.

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 NGI and eDO. 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 application.

User access to information within NGI and the eDO application is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. The eDO is a password protected application, which guards against unauthorized access and disclosure. Before being granted an account, NGI and eDO users are required to attend mandatory training, which further guard against improper access or disclosure of information. Users are trained in the appropriate use and access of the data. Auditing of the application occurs from user logs, monitoring application use, and user activity. 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 privileged 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 or non-work related 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.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: Published federal regulations and Privacy Act notices on the application and appeal forms on the eDO website.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: All information is provided voluntarily by the individual.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: All information is provided voluntarily by the individual.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

With firearms appeals, individuals voluntarily provide personal information to the FBI in order to obtain the reason their firearms purchases were denied, to obtain criminal history records, or to confirm the absence of such records. Because NGI is a biometric-matching system, the individuals may optionally provide fingerprints to confirm identity and to retrieve any criminal history records. The FBI provides notice to the individuals on relevant forms on the eDO website that their personal information will be used for the purposes of confirming identity and to search the reason for the firearms denials.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted. A security risk assessment for NGI, which included the eDO application, was completed on September 28, 2018.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Controls are documented in the NGI Security Traceability Matrix (SRTM).	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Full testing for NGI was conducted on November 26, 2018. The system, including the eDO application, which is within its security accreditation boundary, is further evaluated monthly to ensure safeguards remain in place.	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: NGI's C&A was completed October 23, 2018 and expires October 23, 2021.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: NGI, including eDO, uses the Linux Audit Subsystem and leverages Department of Defense Security Technical Implementation Guides and FBI policy as guidance for what events, access, and measures are audited.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard

Security Controls.]

The eDO application/database inherits the management, operational, and technical controls related to the NGI infrastructure and operating environment. 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. Only authorized FBI personnel and/or contractors may have access to the eDO application. The information is further protected by role-based controls and Access Control List(s) at the group and individual level. Logging and auditing procedures are performed as required.

Please see Sections 3.5 and 4.2 for additional, specific access and security control descriptions. In addition, the NGI system NIST 800-53 security control baseline is at the HIGH impact level of assurance. Security controls are continually assessed during the development life cycle for compliance and to ensure appropriate mitigation strategies have been implemented commensurate with the HIGH impact level of assurance.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Next Generation Identification System 81 Fed. Reg. 27,284 (May 5, 2016) and anticipated modifications to reflect forthcoming updates to the system.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information within the eDO application/database may be retrieved by authorized CJIS personnel via biographic identifiers and/or unique identifying numbers. The criminal history information of those submitting firearms appeals will be retrieved in NGI via fingerprints and information from other CJIS systems will be retrieved via biographic identifiers. All individuals, regardless of citizenship, are entitled to submit firearms appeals to the FBI, and information is not retrieved based on citizenship.