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

Date approved: September 20, 2018

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

EXECUTIVE SUMMARY

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 (DO) 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 Criminal Justice Information Services (CJIS) Division and is known as the "DO process".

In accordance with the regulations, CJIS 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 has submitted this information in hard copy format and CJIS has responded in the same manner. The Electronic Departmental Order (eDO) process is an initiative currently being developed by CJIS and implemented in phases to automate the DO process.

Section 1: Description of the Information System

Current Process:

At this time, CJIS maintains most of the information regarding DO requests in a system called Electronic Fingerprint Conversion (EFCON). EFCON is a subsystem within the FBI's larger Next Generation Identification (NGI) system.[1] The EFCON subsystem maintains original transaction records of NGI for logging and auditing purposes. Unlike the remainder of NGI, EFCON is not searchable by any of the FBI's partners and access and dissemination of information is strictly controlled, even within the FBI.

For the DO process, EFCON maintains all of the Personally Identifiable Information (PII) submitted on the written DO requests, as well as any supplementary documentation that the requesters may choose to send to CJIS, such as letters, legal correspondence, or financial documents. This information is scanned into EFCON and hard copies are destroyed. The requesters' fingerprints are also searched in NGI's fingerprint repositories to determine the existence of criminal history records.

In addition to the information in EFCON, CJIS maintains a DO database on FBInet, a classified FBI system, for the purpose of financial tracking and reconciliation. Only the names and dates of births of the requesters are maintained in this database. CJIS also maintains a database on CJIS UNet, an unclassified FBI system, to resolve requesters' challenges to the accuracy of their criminal history

[1] NGI is the FBI's fingerprint and criminal history system. See, e.g., the privacy impact assessment on Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions, at *https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions*.

records. This database maintains biographic identifiers and associated information.

New eDO Process:

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

An eDO software application and database within NGI will provide the capability for the public to electronically submit the three required components of a DO request (i.e. written request, fingerprints, and payment) and for CJIS to return the criminal history record response in an electronic format. It is expected that this automation will provide more timely and accurate responses to the requesters. The eDO application/database will also largely centralize the DO workflow within the NGI system.

(b) The way the system operates to achieve the purpose.

The eDO application/database hosted on NGI will maintain all DO requests and will replace all existing DO databases. The eDO software application will combine all relevant DO records into a single database that facilitates easy search and retrieval of records. It also will link the electronic DO request, fingerprints, and payment and send a fingerprint search request to the fingerprint repository of NGI.

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

The eDO process will continue to collect the same information from the public that has been collected under the DO process. Requesters typically use the DO application form[2] that requests name, address, citizenship, date of birth, place of birth, physical characteristics, telephone number, email address, prisoner number (if applicable), and the last four digits of the Social Security Number. The requesters will submit this same information electronically on the eDO website.

The requesters must also submit fingerprints because NGI is a biometric system that uses fingerprints to retrieve criminal history and to ensure positive identification. The requesters may also submit financial information related to fee payment, such as credit card or bank account numbers; however, the eDO process will eliminate the collection of much of this financial information by the FBI.

If a criminal history record is located, it will be disseminated to the requester or to his or her designee. Criminal history records typically include additional PII, such as full Social Security Number, race/ethnicity, gender, and alias and maiden names.

(d) Who has access to information in the system.

Access to the eDO application/database will be limited to authorized CJIS and FBI personnel who require access to the information for the performance of their official duties, such as processing DO requests or maintaining information security.

[2] The Applicant Information Form, I-783, is available at www.fbi.gov/services/cjis/identity-history-summary-checks.

(e)How information is transmitted to and from the system.

All hard copy submissions of DO requests, fingerprints, and payments are mailed or faxed to CJIS and CJIS personnel scan the documents into the eDO application/database. DO requests and/or fee payments that are submitted electronically via public websites are secured by the CJIS Shared Enterprise Network (SEN) and FBI Trusted Internet Connectivity Services. The CJIS SEN is a secure telecommunication transport conduit between CJIS systems and the systems to which they connect. The eDO's internet-facing web servers exist within a private Virtual Local Area Network (VLAN) and the data is encrypted while in motion. Fingerprints that are submitted electronically are sent via the CJIS Wide Area Network (WAN), a telecommunications infrastructure that connects authorized agencies to NGI. The purpose of the CJIS WAN is to provide a secure transport mechanism for CJIS criminal history and biometric information. The CJIS WAN transmission hardware is configured by FBI personnel, transmission data to and from CJIS is encrypted, and firewalls are in place.

(f)Whether it is a standalone system or interconnects with other system.

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.

(g) Whether it is a general support system, major application, or other type of system.

The eDO application/database is a major application within the NGI accreditation boundary.

(*h*) *How information in the system is retrieved by the user.*

The eDO public website (www.edo.cjis.gov) will allow requesters to submit electronic DO requests and other documentation for processing by the eDO software application. The public may also use the website to submit challenges to the accuracy or completeness of their criminal history records. The website will return an eDO "Order Number" to the requester as a receipt for a DO submission. The requester also will be provided with a secure link and pin number to access his or her information on the eDO website and to check the status of a request.

For payment, the eDO process will allow a requester to use the U.S. Department of Treasury (Treasury) www.pay.gov website to submit the required fee directly to Treasury. Upon completion of the online application/payment, the requester will receive a payment confirmation email from Treasury, which includes a Treasury confirmation number. A daily activity report from Treasury will be transferred to the eDO software application containing successfully submitted DO request/payment transactions. To complete the request, the individual must submit a copy of the Treasury payment confirmation email, DO request, and fingerprints to CJIS. Once the confirmation email and fingerprints are received, the Treasury confirmation number will be validated by CJIS and the biographic information provided to Treasury will be auto-populated into the eDO database. The use of the Treasury website eliminates the need for CJIS to receive and protect sensitive financial information.

For electronic fingerprints, the requester may submit fingerprints via an authorized government agency

or contractor to NGI. The eDO software application will have the capability to send a fingerprint identification search message to NGI. If the fingerprints match to a criminal history record, that record will be maintained in the eDO database. The eDO software application will provide a formal DO response letter, along with the criminal history record, if applicable. The requester will receive an email notification when the eDO response is ready for retrieval on the website. The response may be provided electronically via the eDO website or mailed via U.S. Postal Service (USPS). The requester will receive a hard copy response if a hard copy request was submitted; a requester may choose either a hard copy or electronic response if an electronic request was submitted. If the fingerprints cannot be processed (e.g. illegible fingerprints), the requester will receive a rejection letter.

CJIS will continue to support the submission of hard copy DO requests, fingerprints, and fees via the USPS. 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. For hard copy requests, fingerprint cards, and fee payments, all documents will be scanned into the eDO database.

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	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 Social Security number is optional and the requester may choose to submit the entire number, the last four digits of the number, or no number. If a criminal history record is located, it will include the full Social Security Number, and be disseminated to the requester or to his or her designee. Also, a unique identifying number in NGI, known as the Universal Control Number, and prisoner number (if applicable) are requested.					

General personal data					
Name	x	Date of birth	x	Religion	
Maiden name		Place of birth	x	Financial info	x
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	

General personal data
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)

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	x	Email	x		
Other (specify): Information is generally not received via telephone; however, CJIS may phone a requester to clarify information or the requester may phone CJIS to request information regarding the DO process.					

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.)

In accordance with the DO regulations, CJIS 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 a monetary fee. CJIS collects only that information which is required by the regulations. This information is necessary to positively identify the individual submitting the request and to perform a fingerprint search of NGI for any criminal history. With the eDO process, CJIS will not maintain hard copy records and will only maintain the information electronically as long as reasonably needed to process a challenge or appeal of the criminal history or to resolve another concern of the requester.

When processing the DO requests manually and returning the criminal history to the requesters via USPS, 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 a DO 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.

Notably, the new eDO process should greatly reduce the possibility of these PII breaches. Although the eDO process will be susceptible to electronic hacking and other security risks, CJIS believes that the system security explained later in this PIA will safeguard against these risks and protect PII much more effectively than the manual process. By using the eDo website, individuals electronically submit DO requests 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 USPS

delivery. The use of a unique pin number to access the eDO website essentially eliminates the possibility of an individual inadvertently accessing another's PII or criminal history. The use of the Treasury's payment website further reduces the risk of an individual's credit card or other financial data from being mishandled.

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 provide access and amendment of criminal history records in compliance with federal regulations		

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 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. In accordance with the regulations, CJIS uses the personal information provided by the requester to confirm identity and to provide a copy of a criminal history record or a finding of no record.

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
	Executive Order	
x	Federal Regulation	28 C.F.R.16.30-16.34

	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, financial information) after three years from the date of processing. The published NARA records schedule is number N1-065-10-16. Hard-copy information may be destroyed immediately once electronically scanned into the system.

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.]

The automation of the DO process greatly improves the security of the personal information submitted by the public and the criminal history records 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. There are approximately 13 roles for eDO users, such as those required for quality assurance, administrative support, and responding to requesters' inquiries. Only CJIS employees who are directly responsible for supporting the DO process will have access to eDO. The eDO application will provide auditing functionality 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 and is verified through audit logs. Audit logs verify what data has been changed, who changed the data, and when the data was changed. 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 only allowed through encrypted communication channels.
n/a	User-Based Collaboration and Information Sharing: eDO is used for dissemination of criminal history records to the requester or designee; it will not be disseminated to others.
x	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 has a 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**.)
x	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 CJIS systems. Secondary storage is via data replication to an offsite datacenter using the ESS. All PII is encrypted while at rest on file storage using a combination of database and file system encryption as appropriate. Data is encrypted in transit to and from the website but only sits at rest on the database, not on the web servers.	

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				
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	x			To the person requesting his or her information. 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 DO request would 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 USPS and several quality control measures are in place to ensure that the information is returned to the correct person. Quality control measures include quality assurance reviews of outgoing responses, and a semi-automated mailing system that prints and places responses in envelopes and provides an address verification screen for the CJIS user. The eDO application will provide the capability for the response to be transmitted electronically via the eDO website and eliminate the possibility of the criminal history and associated PII being lost in the mail.

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 SEN and TIC provide an Internet web proxy service that sits between the eDO requester's web client and the actual eDO service environment. The web proxy service ensures the confidentiality of the requester's information by encrypting the data and the use of certificates on the web proxy service helps to preserve the integrity of the requester's information. The eDO connectivity to the eDO and pay.gov 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 workstation. The workstation runs an NGI operating system baseline that is customized and hardened to accommodate the necessary software. The eDO application leverages NGI's identity management 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. Users receive specific eDO training before accessing the system and also receive information security training annually. 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.

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 statements on the Applicant Information Forms and 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 and the individual is notified of the uses of the information via the Privacy Act statement on the DO request form.
	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 the DO process, individuals voluntarily provide personal information to the FBI in order to obtain their criminal history records or to confirm the absence of such records. Because NGI is a biometric-matching system, the individuals provide fingerprints to confirm identity, as required by the federal regulations. The FBI provides notice to the individuals on the Applicant Information Form and on the eDO website that their personal information will be used for the purposes of confirming identity and to search for criminal history records. In very limited instances, such as when a requester is the subject of an active want or warrant, the FBI may use the information to inform the appropriate law enforcement agency.

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 April 19, 2017.	
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 in August 2013. The system, including the eDO application, which is within its security accreditation boundary, is further evaluated quarterly 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 current C&A expires in October 2018 and a 12 month ATO was granted for eDO on February 2, 2018.	
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. Explanation: No users are authorized outside 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), 82 Fed. Reg. 24151, 156 (May 25, 2017).
	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 individuals will be retrieved.

The criminal history information of those submitting DO requests can only be retrieved in NGI via fingerprint matching. Non-criminal history information within the DO application/database may be retrieved by authorized CJIS personnel via biographic identifiers and/or unique identifying numbers. In addition to the DO request forms, the requesters may choose to submit documentation such as letters, legal correspondence, financial information, immigration status, and court and law enforcement information. All individuals, regardless of citizenship, are entitled to submit DO requests to the FBI.