Federal Bureau of Investigation

Privacy Impact Assessment
for the
Visual Information Support Network (VISNET) and Investigative and Prosecutive Graphic Network (IPGNET)

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: [February 26, 2020]

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

EXECUTIVE SUMMARY

The Visual Information Support Network (VISNET) and the Investigative and Prosecutive Graphic Network (IPGNET) support the Operational Projects Unit (OPU) by providing a system of hardware and software which facilitates the production of visual aids that assist the FBI, state, local, tribal and other federal law enforcement entities with criminal and national security investigations and prosecution.

VISNET and IPGNET are tools of the OPU, located at the FBI Laboratory in Quantico, Virginia. OPU's mission is to provide accurate and responsive technical, photographic, graphic and physical modeling services in support of FBI, state, local, tribal and other federal enforcement investigations and subsequent prosecutions.

OPU personnel receive or collect un-enhanced visual data files from FBI, state, local, tribal and other federal law enforcement investigations. OPU personnel then utilize various software products (e.g., Adobe Photoshop, Adobe Illustrator, Adobe Premier Pro, Adobe After Effects) and air-gapped hardware equipment (e.g., Large Scale Printers, 3D Printers, Laser Cutters) to enhance the data and create final visual products used for investigative and trial aids.

Visual data collected and processed using VISNET and IPGNET describes crime scenes and instruments, victims, suspects, the logistics of criminal schemes (e.g., flowcharts) and special event venues. In addition, data submitted to VISNET and IPGNET may be accompanied by a narrative document that may include the suspect, victim or witness name, address, and other identifiers.

Both VISNET and IPGNET are standalone networks located at the FBI Laboratory in Quantico, VA. They are air-gapped with the instruments that produce the visual aids.

Section 1: Description of the Information System

Provide a non-technical overall description of the systems that addresses:

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

The purpose of the Visual Information Support Network (VISNET) and the Investigative and Prosecutive Graphic Network (IPGNET) is to support the Operational Projects Unit (OPU) by providing a system of hardware and software which facilitates the production of visual aids that assist the FBI, state, local, tribal and other federal law enforcement entities with criminal and national security investigations and prosecution.

VISNET is used for the production of unclassified materials, whereas IPGNET is used for the processing of classified products.

(b) the way the systems operate to achieve the purpose(s);

OPU personnel receive or collect un-enhanced visual data files from FBI, state, local, tribal and other federal law enforcement investigations. OPU personnel then utilize various software products (e.g., Adobe Photoshop, Adobe Illustrator, Adobe Premier Pro, Adobe After Effects) and air-gapped hardware equipment (e.g., Large Scale Printers, 3D Printers, Laser Cutters) to enhance the data and create final visual products used for investigative and trial aids. VISNET and IPGNET run both Apple and Microsoft operating systems to accommodate various file types and software applications. Neither VISNET nor IPGNET run any mail or instant messaging software.

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

Visual data collected and processed using VISNET and IPGNET describes crime scenes and instruments, victims, suspects, the logistics of criminal schemes (e.g., flowcharts) and special event venues, and includes:

- photographs;
- 3-D modeling;
- aerial imagery;
- enhanced surveillance videos and audio files;
- Computer based animation (e.g., age progressions); and
- composite sketches.

In addition, data submitted to VISNET and IPGNET may be accompanied by a narrative document that may include the suspect, victim or witness name, address, and other identifiers.

The systems also collect User Logon ID and the date/time of activity.

All information received, as well as all products generated, is stored on VISNET and IPGNET network folders, which are named as sequential work order numbers.

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

OPU team members are assigned a unique VISNET user ID and password by VISNET system administrators upon completing a Security Access Request (SAR), which requires System Owner and system Information System Security Officer (ISSO) signature approval, and signing a Rules of Behavior (RoB) Acknowledgement Form, which the system ISSO will also sign.

Like VISNET, access is granted to IPGNET by IPGNET system administrators upon completion of a SAR and RoB Acknowledgment Form, with System Owner and system ISSO approval. However, due to the smaller volume of classified cases, unlike VISNET, only a limited number of OPU team members are granted an IPGNET user ID and password.

Users login to either VISNET or IPGNET using their corresponding user name and password to access the system's data stores. User names and passwords are unique to each system.

VISNET and IPGNET user access is logged and is subject to weekly audits by the VISNET and IPGNET Information System Security Officer and System Administrator. The audits look for anomalies in the system security logs, such as failed login attempts and after normal business hour logins. User accounts are disabled immediately when VISNET and/or IPGNET personnel are no longer actively employed by the program or are found to be using information inappropriately.

Privileged users are the VISNET and IPGNET System Administrators, who have access to the servers as well as the files. The System Administrators are responsible for the upkeep, configuration and reliable operation of VISNET and IPGNET. Actions taken by the privileged users are captured by the security logs, which are reviewed by the systems' ISSO every 7 calendar days as part of the overall system security and process logs audit. Like general users, privileged users also must complete a Security Access Request, which is signed by both the System Owner and ISSO, and sign a RoB Acknowledgement form. Additionally the privileged users must complete annual mandatory Privileged User Security training through Virtual Academy[1] to maintain their level of system access. This training provides privileged users with information security risks associated with their daily activities and their responsibilities in complying with FBI policies and the RoB. Additional mandatory training offered via Virtual Academy includes Information Security (INFOSEC) Awareness and privacy training. Proof of completion of training is maintained in Virtual Academy.

Media (CDs, USBs, etc.) are only used within the Operational Projects Unit's (OPU) spaces within the FBI Laboratory Facility and are not distributed to anyone outside OPU or to anyone who does not have access to VISNET or IPGNET. Information is not electronically distributed.

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

Generally, users access the data by work order number, however, some raw data files within the numbered folders may be given names by the contributing law enforcement entity that include victim or subject name or other personal identifier. In these instances data could theoretically be accessed by personal identifier, but this is not the typical use case. In addition, graphic information may contain personally identifying elements, but in practice, users do not search the contents of information for personal identifiers.

Due to the collaborative nature of the work, and the need to provide continuity of operations should team members be deployed to other assignments, all OSU users are able to view and update all data contained within all work orders. Information contained within work orders includes both in-progress and completed photographs; 3-D modeling; aerial imagery; enhanced surveillance videos and audio files; computer based animation (e.g., age progressions); and composite sketches.

[1] (U) Virtual Academy is the FBI's training system, and is covered by separate privacy documentation.

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

Data from FBI, state, local and other federal law enforcement investigations is acquired via portable removable electronic storage media, e.g., thumb drives, compact disks (CDs), hard drives. Finished visual products are returned using the same array of electronic media. For FBI products, the investigative case agent is responsible for Sentinel recordkeeping.

(g) Whether they are standalone systems or interconnect with other systems (identifying and describing any other systems to which it interconnects).

Both VISNET and IPGNET are standalone networks located in Quantico, VA. They are air-gapped with the instruments that produce the visual aids.

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			
Note: While it is theoretically possible that a Social Security Number (SSN) could be included in the narrative file or part of an image presented for enhancement, such an occurrence would be atypical. As general rule, SSNs are not collected, maintained or disseminated from IPGNET or VISNET.					

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

Work-related data					
Occupation		Telephone number	X	Salary	

Job title		Email address		Work history	
Work address		Business associates			

Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other information (specify)					
None.					

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

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

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign			

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					

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 privacy risks associated with the type, quantity, and sources of information collected are over-

collection, unauthorized access and misuse. These risks are minimized by access and security controls, as follows.

- The risk of over-collection of data is mitigated by the limited nature of information provided by the investigative authorities for processing.
- User access is role-based. Not all users have access to all data.
- Physical access to the server is limited to the System Administrators, who receive privileged user training on an annual basis.
- Only System Administrators can make configuration changes to the system. General users do not have permission to make configuration changes.
- All access is password-protected.
- Users are required to take the INFOSEC Awareness and privacy training on an annual basis.
- VISNET and IPGNET are standalone systems; remote and mobile access is not applicable
- User groups are established by the System Owner based on a defined need to know and a role requiring access to the data.
- VISNET and IPGNET user access is logged and audited on a weekly basis for activity. Any anomalies are analyzed to determine if the action was benign or malicious in intent. The audit features are fully documented in the System Security Plan (SSP).
- User accounts are disabled immediately when VISNET and/or IPGNET personnel are no longer actively employed by the program or are found to be using information inappropriately.
- Vulnerability scans of VISNET and IPGNET are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.

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			
X	For criminal law enforcement activities		For civil enforcement activities
X	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
X	For litigation (for criminal prosecutions)		
	Other (specify):		

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.

The information is collected, maintained and disseminated in furtherance of the FBI's mission to investigate crimes and assist state, local and other federal law enforcement, as it enables the FBI to describe / display crime scenes and instruments, victims, suspects, the logistics of criminal schemes (e.g., flowcharts) and special event venues for investigative and prosecutorial purposes.

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. 533
X	Executive Order	E.O. 12333
X	Federal Regulation	28 C.F.R. 0.85
	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.)

All records and products are currently being retained, pending NARA approval of a proposed 30-year disposition schedule.

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.)

Privacy risks associated with access to VISNET and/or IPGNET and the data produced include the possibility of data being mishandled or users viewing data which they are not authorized to view. These risks are mitigated in several ways such as the following:

- VISNET and IPGNET are maintained in physically controlled environment.

- Prior to granting access to VISNET and/or IPGNET, users must complete a SAR and sign a RoB Acknowledgement Form.
- Access is limited to personnel who have a VISNET and or IPGNET desktop or laptop computer and that access is role-based. Not all users have access to all data.
- Physical access to the server is limited to the System Administrators, who receive privileged user training on an annual basis. Proof of completion of training is maintained in Virtual Academy.
- Only System Administrators can make configuration changes to the system. General users do not have permission to make configuration changes.
- All access is password-protected.
- Users are required to take the INFOSEC Awareness and privacy training on an annual basis. Proof of completion of training is maintained in Virtual Academy.
- VISNET and IPGNET are standalone systems; remote and mobile access is not applicable
- User groups are established by the System Owner based on a defined need to know and a role requiring access to the data.
- VISNET and IPGNET user access is logged and audited on a weekly basis for activity. Any anomalies and/or unusual activities is analyzed to determine malicious intent. The audit features are fully documented in the System Security Plan (SSP).
- User accounts are disabled immediately when VISNET and/or IPGNET personnel are no longer actively employed by the program or are found to be using information inappropriately.
- Vulnerability scans of VISNET and IPGNET are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.

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.

IPGNET processes classified information and therefore meets the NIST 800-59 definition of a National Security System. VISNET does not process classified information and so does not meet the definition.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to

	access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
N/A	Remote Access: remote access is prohibited or limited to encrypted communication channels.
N/A	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements.
N/A	Access Control for Mobile Devices: access to PII is prohibited on mobile devices or limited so that data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.
VISNET and IPGNET are standalone systems; Remote access, User-Based Collaboration and Information Sharing and Access Control for Mobile Devices is not applicable as these scenarios are not permitted within the confines of VISNET and IPGNET.	

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 is prohibited.

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.
Media (CDs, USBs, etc.) are only used within the Operational Projects Unit's (OPU) spaces within the FBI Laboratory Facility and are not distributed to anyone outside OPU or to anyone who does not have access to VISNET or IPGNET. Information is not electronically distributed.	

Data Confidentiality controls (Be sure to also discuss in Section 1(f).)

N/A*	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**.)
*VISNET and IPGNET are standalone networks. OPU is evaluating 3rd party encryption software.	

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			
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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.)

The privacy risk associated with disclosure or sharing of information is the risk of misuse. In addition to the mitigations set forth in Sections 2.3 and 3.5, the risk of unauthorized disclosure is mitigated by the FBI's Domestic Investigations and Operations Guide (DIOG), which proscribes sharing and disclosure of data except in furtherance of a lawful purpose and mission-appropriate review and pre-approval.

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.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: The system contains data potentially relevant to a predicated investigation. If individuals were given notice of the investigation, the utility of the system and any investigative activity would be diminished.

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

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: The system contains data potentially relevant to a predicated investigation. If individuals were given notice of the investigation, the utility of the system and any investigative activity would be diminished.

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.

Notice of the collection and uses of the information in the system is provided in the published System of Records Notices (SORNs) set forth in Section 7.1. This SORN provides general notice regarding the entities with and situations in which the FBI may use and disseminate the records in this system. The published routine uses and blanket routine uses applicable to this system provide additional notice about the ways in which information maintained by the FBI may be shared with other entities.

As explained in Section 5.2, the FBI does not provide notice and an opportunity to consent that is more specific. The information in this system is collected by the FBI in furtherance of authorized investigative activities. It is therefore not possible to provide individuals with notice and an opportunity to consent to the collection of their data, as doing so could jeopardize FBI investigations, compromise intelligence or law enforcement sources and methods, and result in harm to US citizens and national security.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The System implements all applicable DOJ/FBI Core Security Controls for FISMA compliance, and, as set forth in Sections 2.3 and 3.5, applies appropriate security controls to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient.

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: The System Owner establishes, administers and monitors the use of user accounts in accordance with a role-based access determination that organizes authorized access and privileges into roles. All users are authorized by the System Owner using the FBI SAR process available through the FBI EPAS business process manager tool. The system inherits the monitoring and reporting of information system accounts for atypical use in accordance with the Security Monitoring of FBI Information Systems Policy Guide, 0655PG-3, from the FBI Enterprise Security Operations Center (ESOC) as part of their enterprise charter. The System Owner monitors, at least annually, privileged role assignments for the System. Additionally, the System Program Manager and ISSO review user accounts in comparison to the audit log table export and Active Directory Global Access List. The system takes disabling (or revocation) actions when privileged role information system account assignments are no longer appropriate in accordance with FBI procedures indicated Both IPGNET and VISNET conduct quarterly vulnerability assessments and weekly audits of security logs.
*	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: *IPGNET and VISNET currently do not have Authorization to Operate (ATO). This authorization is currently underway. The ATOs for VISNET and IPGNET are expected by Q1 FY2020.
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: The System inherits from the FBI ESOC the employment of automated mechanisms to integrate audit review, analysis, and correlation of audit records across different repositories to gain FBI-wide situational awareness and reporting to support organizational processes for investigation and response to suspicious activities. Moreover, the System ISSO and System Administrator review and analyze the audit records at least every seven (7) calendar days for indications of inappropriate or unusual activity and reports findings to designated FBI personnel with security roles.
N/A	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. Operational Projects Unit personnel, the users of IPGNET and VISNET, are government employees. Contractors are not system users.
N/A	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy. Operational Projects Unit personnel, the users of IPGNET and VISNET, are government employees. Contractors are not system users.
X	The following training is required for authorized users to access or receive information in the system:

	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.

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.]

As set forth in Sections 2.3 and 3.5, access and security controls are utilized to protect privacy and reduce the risk of unauthorized access and disclosure, as follows:

- User access is role-based. Not all users have access to all data.
- Physical access to the server is limited to the System Administrators, who receive privileged user training on an annual basis.
- Only System Administrators can make configuration changes to the system. General users do not have permission to make configuration changes.
- All access is password-protected.
- Users are required to take the INFOSEC Awareness and privacy training on an annual basis.
- VISNET and IPGNET are standalone systems; remote and mobile access to is not applicable
- User groups are established by the System Owner based on a defined need to know and a role requiring access to the data.
- VISNET and IPGNET user access is logged and audited on a weekly basis for activity. Any anomalies and/or unusual activities is analyzed to determine malicious intent. The audit features are fully documented in the System Security Plan (SSP).
- User accounts are disabled immediately when VISNET/IPGNET personnel are no longer actively employed by the program or are found to be using information inappropriately.
- Remote and mobile device access to IPGNET and VISNET is prohibited.
- Vulnerability scans of VISNET and IPGNET are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.

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:

	FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017); DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (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 United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Users will then access the data by work order number. (Some raw data files within the numbered folders may be given names by the contributing law enforcement entity that include victim or subject name or other personal identifier. In these instances data can be accessed by personal identifier, but this is not the typical use case.) In addition, graphic information may contain personally identifying elements, but in practice, users do not search the contents of information for personal identifiers.