Federal Bureau of Investigation

Privacy Impact Assessment
for the
FBI Police Automated Security Roster (ASR)

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: October 3, 2019

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

EXECUTIVE SUMMARY

The FBI Police Automated Security Roster (ASR) is a web-based application on the FBI Network (FBINet) that automates the Duty Roster, Visitors Notification System (VNS), and Daily Patrol information. All ASR subsystems are accessible via FBINet at all FBI locations. The Duty Roster tracks daily FBI Police patrol assignments; the VNS contains information about all visitors (Bureau and non-Bureau) to FBI space; and the Daily Blotter is a daily log, by location, of police activities, including lost and found events.

The data includes records of police assignments by FBI location; a daily events log by location and day; detailed event information by FBI location; visitor information; and a record of items lost and found around FBI facilities.

FBI Police Officers with a valid FBINet user identification (Id) and password are permitted to create, read, edit and print their own records in all ASR subsystems (VNS, Duty Roster, and Daily Blotter). Senior FBI Police Officers can read, edit and print all records in all subsystems.

In addition, all FBI employees, contractors and detailees (FBI personnel) with a valid FBINet user Id are permitted to create, read, edit and print their own records in VNS, but only FBI Unit Chiefs are permitted to approve VNS records.

This PIA was conducted because the VNS and Daily Blotter subsystems collect and maintain personally identifiable information (PII) of U.S. persons.

Section 1: Description of the Information System

Provide a non-technical overall description of the system. Your responses should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

(a) Purpose that the records and/or system are designed to serve:

The FBI ASR automates the Duty Roster, VNS, and Daily Patrol information and is accessible via FBINet[1] at all FBI locations. A web-based application on FBINet, the ASR is comprised of three subsystems: the Duty Roster, the VNS and the Daily Blotter. The Duty Roster tracks daily FBI Police patrol assignments; the VNS contains information about all visitors (Bureau and non-Bureau) to FBI space; and the Daily Blotter is a daily log, by location, of police activities, including lost and found events.

[1] FBINet is the primary network for the daily investigative and administrative functions of the FBI and is located on the FBI's Secret Enclave. FBINet is covered by separate privacy documentation.

(b) Way the system operates to achieve the purpose(s):

FBI police officers logon to ASR via a web browser on FBINet where they must enter a user Id and password and select the Acknowledgement box agreeing to abide by the terms and conditions displayed on the logon screen. After logging-in to ASR, FBI police officers can access all ASR subsystems. In addition to being part of ASR, VNS is separately accessible to all FBI personnel via a web browser on FBINet.[2] Once the client has logged-in to ASR successfully, a screen is presented that displays a menu of the ASR subsystems (Duty Roster, Visitors Notification System (VNS), and Daily Patrol). After the desired subsystem is selected, a new screen is presented displaying the options for working with the data for that subsystem. For example, if the 'Duty Roster' option is chosen, a screen is displayed allowing the client to enter elements such as Name, SSN, Work Location, Work Schedule etc. If the client selects the "Submit" option, the data entered is stored in the database. In the case of reporting options, the client enters the report parameters, such as the report and date range, hits enter and the report is displayed.

(c) Type of information collected, maintained, used, or disseminated by the system:

The data includes records of police assignments by FBI location; a daily events log by location and day; detailed event information by FBI location; visitor information; and a record of items lost and found around FBI facilities. The ASR contains information dating back to 1997.

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

FBI Police Officers with a valid FBINet user Id and password are permitted to create, read, edit and print their own records in all ASR subsystems (VNS, Duty Roster, and Daily Blotter). Senior FBI Police Officers can read, edit, and print all records in all subsystems.[3]

Access to edit and create data is based upon the facility to which the police officer belongs (e.g., officers stationed at Quantico cannot enter data for officers stationed at the Criminal Justice Information Services (CJIS) Division). Moreover, police officers cannot edit records that they did not enter into the system. However, for the safety and security of FBI personnel and facilities, any police officer can query all ASR records. Types of inquiries include:

- Did a suspicious person logged at Quantico attempt entry into any of the other facilities?
- How often are CJIS security alarms triggered? During what hours of the day? Is the same happing in New York? Could this be a malicious actor attempting to test our security alarms?
- What is the frequency to which Quantico Police Sergeants are assigned to posts as compared to CJIS?

---

[2] After the ASR System was developed, it became apparent that non-police personnel have a need to access visitor information. Thus a separate access point was established to enable non-police personnel to access VNS data. There is one VNS, but with two different points of entry.

[3] Senior FBI Police Officers include those personnel with the rank of Corporal, Sergeant, Lieutenant, Captain, Major, or Unit Chief.

In addition, all FBI personnel (not just FBI Police Officers) with a valid FBINet user Id are permitted to create, read, edit and print their own records in VNS, but only FBI Unit Chiefs are permitted to approve VNS records.

Although all ASR subsystems are accessible via FBINet at all FBI locations, currently only FBI Police Officers at the following locations access the Duty Roster and Daily Blotter:[4]

- FBI Headquarters (HQ);
- Washington Field Office (WFO);
- CJIS Division;
- New York Field Office (NYFO); and
- FBI spaces at Quantico, VA.

Similarly, VNS is currently accessed by FBI personnel at the following locations:[5]

- HQ;
- WFO;
- CJIS Division;
- NYFO;
- Quantico;
- Oklahoma City Field Office;
- LEGAT-Brussels/Belgium;
- Baltimore Field Office;
- Terrorist Screening Center;
- Little Rock Field Office;
- Oklahoma City Field Office; and
- Indianapolis Security Office.

(e) How information in the system is retrieved by the user:

Users access ASR to input and retrieve information via a web page on the FBINet Intranet.[6] Users are required to logon to ASR (or VNS) with a valid FBINet user Id and password. Password validation is provided by Windows Active Directory.[7] Once users have successfully logged-in to ASR, they are presented with a menu of ASR subsystems (Duty Roster, Visitors Notification System (VNS), and Daily Patrol) to select from. When the desired subsystem is selected, a new screen is displayed with options for that subsystem.

(f) How information is transmitted to and from the system:

---

[4] Please note that this is subject to change since the ASR is accessible to all FBI personnel with the proper credentials.
[5] This is also subject to change since the ASR is accessible to all FBI personnel with the proper credentials.
[6] VNS is accessible through its own FBINet Intranet address, or through ASR.
[7] Windows Active Directory is a set of processes that authenticates and validates user access to FBINet.

FBI Police Officers with a valid FBINet user Id and password are permitted to create, read, edit and print their own records in all ASR subsystems (VNS, Duty Roster, and Daily Blotter). Senior FBI Police Officers can read, edit and print all records in all subsystems.

In addition, all FBI personnel (not just FBI Police Officers) with a valid FBINet user Id are permitted to create, read, edit, and print their own records in VNS, but only FBI Unit Chiefs are permitted to approve VNS records.

Daily Blotter users can generate police activity reports for a selected date range. VNS users can generate reports by selecting the elements they want displayed from a selection of data elements such as Visitor Name. Duty Roster users can create reports based on duty shift and date range.

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

ASR interfaces with Window's Active Directory for User Authentication. VNS (separately or within ASR) interfaces with the Human Resources (HR) Source[8]/FBI Personnel Locator Table, which links all FBI personnel to a physical location. This validates if a visitor is FBI personnel.

Section 2: Information in the System

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

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

Identifying numbers					
Social Security	R, B	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card		Security Badge	V
Other identifying numbers (specify): Badge Number [R, B], Badge Type [R, B], Visitor Number [V]					

General personal data					
Name	R, B, V	Date of birth		Religion	
Maiden name		Place of birth		Financial info	

[8] HR Source Reports is the official FBI-wide application for viewing HR information. HR Source is covered by separate privacy documentation.

General personal data					
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): None.					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): Shift [R], Shift Date [R], Police Narrative [B], Police Post Assignments (location) [R], Police assigned to Post (names) [R]					

Distinguishing features/Biometrics					
Fingerprints				DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): None.					

System admin/audit data					
User ID	R, B, V	Date/time of access	R, B, V	ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify): None.					

Other information (specify)
Event data, Visiting Location [V], Purpose of Visit [V], Visitor's Sponsor [V], Visitor arrival time [V]

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

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

Directly from individual about whom the information pertains						
In person		B	Hard copy: mail/fax		Online	
Telephone			Email			
Other (specify): None						

Government sources

Within the Component	R, B, V	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify): None					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): None					

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 type, quantity, and sources of information collected are necessary and narrowly tailored to support visitor vetting (VNS), daily FBI police patrol assignments (Duty Roster), and a log of police officer activities (Daily Blotter). The privacy risks associated with the information collected are unauthorized access, breach, and misuse. These risks are minimized by the following access and security controls.

- User access is role-based. Not all users have access to all data.
- Physical access to the server is limited to the ASR Administrator, who receives 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. Each user must enter a user ID and password before logging on to ASR.
- FBI personnel receive annual privacy and information assurance training to inculcate a user culture that militates against the misuse of PII.
- Users are required to take security and privacy training on an annual basis.
- The System inherits from ESOC the employment of automated mechanisms to integrate audit review, analysis, the analysis and correlation of audit records across different repositories to gain FBI-wide situational awareness, the analysis and correlation of audit records across different repositories to gain FBI-wide situational awareness and reporting processes to support organizational processes for investigation and response to suspicious activities. Moreover, the System ISSO and Program Manager review and analyze the audit records every seven days for indications of inappropriate or unusual activity and reports findings to designated FBI personnel with security roles.

User groups are established by ASR management based on a defined need to know and a role requiring access to the data.

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.)

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

Purpose			
R, B	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	R, B, V	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		
	Other (specify): None		

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 that is collected, maintained, and disseminated is necessary to support the VNS, Duty Roster, and Daily Blotter processes.

- VNS provides an orderly process for FBI personnel to schedule visitors to FBI space, and for positive Id of all visitors.
- The Duty Roster enables the FBI to ensure an appropriate on-premises police presence.
- The Daily Blotter permits oversight and accountability of FBI police activity.

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. 33, Sec. 533 (authorizing the Attorney General the authority to "detect and prosecute crimes against the United States)."
	Executive Order	
X	Federal Regulation	28 C.F.R. 0.85(a) (generally giving the FBI jurisdiction to investigate violations of all laws).
	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.)

Information in the ASR will be destroyed 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use. See General Records Schedules DAA-GRS-2017-0006-0001; DAA-GRS-2017-0006-0005; and DAA-GRS-0006-0013.

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.)

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.

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.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	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.
X	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.

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.
NA	Media Transport: media is encrypted or stored in a locked container during transport.
NA	Media Sanitation: media is sanitized prior to re-use.
[The transfer of data outside of ASR to any Media is prohibited.]	

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

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**.)

Information System Monitoring

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

The privacy risks associated with using the information in ASR include unauthorized access, mishandling or loss of data, and inaccuracy of information. These risks are minimized by the following access and security controls.

- User access is role-based. Not all users have access to all data.
- Physical access to the server is limited to the ASR Administrator, who receives 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.
- FBI personnel receive annual privacy and information assurance training to inculcate a user culture that militates against the misuse of PII.
- Users are required to take security and privacy training on an annual basis.
- User groups are established by ASR management based on a defined need to know and a role requiring access to the data.
- ASR requires 2-factor authentication. Users are automatically timed-out after 30 minutes of inactivity. In addition, regular auditing is performed to determine unauthorized access.

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.

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			R, B, V	
DOJ components	R, B			
Federal entities	R, B,			
State, local, tribal gov't entities	R, B			
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 risks associated with disclosure or sharing of information are the risks of unauthorized access and disclosures. Therefore, all users must acknowledge the following terms and conditions before logging on:

Computer Use Policy (Warning Banner)

- FBINET computers are accredited to the Secret level ONLY. Transmitting, processing, or storing Top Secret and SCI data on FBINET computers is PROHIBITED.

WARNING!

- You are accessing a U.S. Government information system, which includes: (1)this computer,(2)this computer network,(3)all computers connected to this network, and(4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.
- By using this information system, you understand and consent to the following:
    - You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system.
    - Any communication transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

In addition to the controls set forth in the instant paragraph, and in Sections 2.3 and 3.5, ASR has implemented the National Institute of Standards and Technology (NIST) 800-53 Recommended Security Controls for Federal Information Systems controls, which are referenced in NIST 800-122, Guide to Protecting the Confidentiality of PII. This minimizes the risk that information is disclosed or accessed in an unauthorized manner.

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.)

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

R, B, V	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.

In the following tables, R = Duty Roster; B = Daily Blotter; and V = VNS.

B	Yes, individuals have the opportunity to decline to provide information.	Specify how: Members of the public have the right to remain silent when confronted by an FBI police officer.
R, V	No, individuals do not have the opportunity to decline to provide information.	Specify why not: The information in the Duty Roster and VNS subsystems pertains to internal government operations.

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:
R, B, V	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: The information in the Duty Roster and VNS subsystems pertains to internal government operations. The information in the Daily Blotter is potentially relevant to authorized investigative activity. If individuals were given notice of the investigation, the utility of the system and any investigative activity would be diminished. Therefore, they do not have the opportunity to consent to particular uses of the information.

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 Notice (SORN) 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 law enforcement and/or national security 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 as set forth in Table 1. All users are authorized by the System Owner using the FBI System Access Request process available through the FBI Enterprise Process Automation System business process manager tool. The system inherits the monitoring and reporting of information system accounts for atypical use in accordance with FBI Enterprise Security Operations Center (ESOC) policy 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.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: May 2018 (expires 9/25/2019)

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, the analysis and correlation of audit records across different repositories to gain FBI-wide situational awareness, the analysis and correlation of audit records across different repositories to gain FBI-wide situational awareness and reporting processes to support organizational processes for investigation and response to suspicious activities. Moreover, the System ISSO and Program Manager review and analyze the audit records every seven days for indications of inappropriate or unusual activity and reports findings to designated FBI personnel with security roles.	
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.]

Many of the access and security controls to protect privacy and reduce the risk of unauthorized access and disclosure have already been discussed in Sections 2.3, 3.5, and 4.2. Generally, however, to mitigate potential risks, ASR has implemented managerial, operational, and technical security controls consistent with DOJ Order 2640.2E (or successor) and associated information technology security standards, which are derived from NIST 800-53, Recommended Security Controls for Federal Information Systems, and the Federal Information Security Management Act.

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: Justice/FBI-008, Bureau Personnel Management System (BPMS), 58 Fed. Reg. 51, 875 (Oct. 5,

	1993), as amended at 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017); DOJ-002, DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), as amended at 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.

Information in ASR, including information about United States Persons, can be retrieved by a keyword search of any ASR field, but would most likely be retrieved by some combination of any or all of the following identifiers:

- Social Security #;
- Name;
- Telephone #;
- Work Address; and
- User Id.