Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Phoenix Platform]

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

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

Date approved: [Component to insert date of PIA approval]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Phoenix Platform (Phoenix) collects, maintains and disseminates information required for background investigations, physical access, and security clearances for FBI employees, contractors and detailees (collectively, personnel), visitors and applicants. Phoenix also provides a self-service portal. Within the self-service portal, FBI personnel can request access to Phoenix, submit Phoenix troubleshooting requests, request and access North Atlantic Treaty Organization (NATO) clearance read-in materials, and view all active FBI Special Investigators (SIs).[1] FBI contractors can use the self-service portal to update their contact information. Phoenix also generates Unique Employee Identification numbers (UEIDs)[2] for all FBI employees.

Section 208 of the E-Government Act of 2002, P.L. 107-347 requires that agencies conduct Privacy Impact Assessments (PIAs) on information technology systems that collect and maintain identifiable information regarding individuals, and, if practicable, to make such PIAs publicly available. Accordingly, this PIA has been conducted and will be made publicly available. As changes are made to Phoenix, this PIA will be appropriately reviewed and revised.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

Phoenix is a web-based FBI Secret Enclave (FBINet) application that collects, maintains and disseminates information required for background investigations, physical access, and security clearances for FBI personnel, visitors and applicants. Phoenix is used primarily by the FBI Security Division (SecD), but is accessible to all FBI personnel on a need to know basis. Within the self-service portal, FBI personnel can request access to Phoenix, submit Phoenix troubleshooting requests, request and access North Atlantic Treaty Organization (NATO) clearance read-in materials, and view all active FBI Special Investigators (SIs). FBI contractors can use the self-service portal to update their contact information. Phoenix also generates Unique Employee Identification numbers (UEIDs)

[1] SIs are responsible for conducting background investigations on applicants for employment with the FBI and other federal agencies, and on current federal employees who require investigations or reinvestigations for security clearances. Phoenix displays SI name, home phone, home city, home state, home zipcode, start date, and credential expiriation date. SIs are federal contractors who hold a Top Secret security clearance. The active SI report is made available to all FBI personnel because anyone in the FBI may receive a call from an outside entity to verify that the person who contacted them is actually an SI working on behalf of the FBI.

[2] A UEID is a less privacy-intrusive alternative to a Social Security Number.

for all FBI employees. Phoenix's predecessor, the Facility Security System (retired), was a component of the Bureau Personnel Management System (BPMS)/Enterprise Application Services Program (EASP), and Phoenix is contained within the EASP system boundary.[3]

Users logon to Phoenix by entering its Uniform Resource Locator (URL) into an FBINet workstation web browser. Authentication and single-sign-on are provided by FBINet Active Directory. Upon access, users are presented with a menu of request, entry and search options, based on their role and associated permissions.

By default, anyone with a valid FBINet ID can access the self-service capabilities provided by Phoenix's self-service portal. Additional Phoenix access permissions, as set forth below must be approved by the requestor's chain of command and SecD.

- **Limited Background Investigators** can add and edit background information for individuals who do not require a security clearance, such as building service contractors (e.g., window washers).

- **SecD Personnel** (including **Security Officers**) can add and edit clearance, access, and background investigation information, view and edit physical and system access information, and generate Financial Disclosure reports for FBI personnel with access to Sensitive Compartmented Information.

- **Information Management Division Name Check Program Personnel** can view clearance, background investigation, facility access and system access records.

- **Contracting Officer Representatives (CORs)** can add and update contract related information for FBI contractors entering FBI-space on a Visit Access Request.

- **System Administrators** (who are SecD and Finance Division personnel) can approve system access requests. SecD System Administrators can also perform system update, troubleshooting and maintenance activities.

Phoenix also allows users to serialize documents to Sentinel,[4] print pre-defined and custom reports, and export data for use in external applications such as Microsoft Excel. All users can generate reports and data exports of the information to which they have access.

Information can be retrieved from Phoenix by searching any field to which the user has access. Information is transmitted from Phoenix by reports and data exports, and via interconnections with the following systems:

---

[3] EASP is the subject of separate privacy documentation.

[4] Sentinel is the FBI's case management system, and is the subject of separate privacy documentation.

- The Enterprise Process Automation System (EPAS), which is the FBI's internal system for documenting and tracking FBI personnel requests for access to various FBI systems and programs,[5] to retrieve background investigation status;

- HR Source, to transmit employee UEIDs, and retrieve employee identifying information (e.g., first name, last name, date of birth, etc.); and

- The FBI Insider Threat Referral System (ITRS),[6] to transmit identifiers for non-employee personnel.

Employee identifiers and descriptive information is transmitted to Phoenix by HR Source, which is the FBI's human resources system.[7] Background investigation status information is transmitted to Phoenix by EPAS.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	5 U.S.C. §§ 301, 1104, 1302, 3109, 4103, 4305 and 7201; 5 U.S.C. §§ 3301, et seq.; 18 U.S.C. § 3771; 28 U.S.C. § 533; 29 U.S.C. § 701, et seq.; 34 U.S.C. § 20141; 41 U.S.C. § 523; 42 U.S.C. § 2000e-16.
Executive Order	E.O. 9397; E.O. 10450; E.O. 10865; E.O. 12333; E.O. 12564; E.O. 12968; E.O. 13356. E.O. 13388; E.O. 13526; E.O. 10450.
Federal regulation	28 C.F.R. § 0.85(b); 5 C.F.R. §§ 410.201; 5 C.F.R. §§ 410.301; 29 C.F.R. § 720.301, et seq.;

[5] EPAS is the subject of separate privacy documentation.

[6] ITRS is the subject of separate privacy documentation.

[7] HR Source is the subject of separate privacy documentation.

	48 C.F.R. (FAR); 48 C.F.R. § 2801.
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	
Date of birth or age	X	A, B, C, and D	
Place of birth	X	A, B, C, and D	
Gender			
Race, ethnicity or citizenship	X	A, B, C, and D	Citizenship only
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Full SSN
Tax Identification Number (TIN)	X	A	For contractors, If applicable
Driver's license	X	A, B, C, and D	
Alien registration number			
Passport number	X	A and D	
Mother's maiden name			
Vehicle identifiers			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal mailing address	X	C	SI city, state, and zipcode
E-mail addresses (personal, work, etc.) Please describe in Comments	X	A	Work and personal email addresses
Phone numbers (personal, work, etc.) Please describe in Comments	X	A, B, C, and D	Work and personal phone numbers
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	A	
Applicant information	X	C	
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Procurement/contracting records	X	A	Information relevant to contract employee building and security access
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**	X	A	
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			
- **Passport Expiration Date**	X	A and D	
- **Passport Issuing County**	X	A and D	
- **UEID**	X	A	
- **Case File Number**	X	A	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Cease Duty Date**	X	A	
- **Position Title**	X	A	
- **Entry On Duty Date**	X	A	
- **Person Type**	X	A, B, C and D	Values include Agent, Applicant, Contractor, Detailee, Official Visitor, Private Sector, etc.
- **Person Status**	X	A	Values are Active, Denied, Inactive, Suspended and Terminated
- **Division**	X	A	
- **Cost Code**	X	A	
- **Company**	X	A, B, C and D	
- **Company Address**	X	A, B, C and D	
- **Clearance**	X	A, B, C and D	Values are Secret and Top Secret
- **Polygraph**	X	A	Values are Full Scope Polygraph and Personnel Security Polygraph
- **SCI Access**	X	A	Values are SI, TK, HCS, G, and HCSP
- **Investigations**	X	A	Values are Secret, Top Secret, and Single Scope Background Investigation (for SCI)
- **Validations**	X	A	Values are Deactivated, Pending, and Validated
- **Communications Security Access**	X	A	
- **Security Exceptions**	X	A	Values are Condition, Deviation, Out of Scope, and Waiver
- **Organization**	X	A, B, C and D	
- **Cost Center**	X	A	
- **Field Office Resident Agency Code**	X	A	
- **Squad Code**	X	A	
- **Supervisor Position**	X	A	
- **Supervisor / POC**	X	A	
- **Contracting Officer Representative (COR) Name**	X	A	
- **Building Name**	X	A, B, C and D	
- **Access Type**	X	A	Values are Escorted and Unescorted
- **Room Number**	X	A, B, C and D	
- **Computer Access**	X	A	Values are Yes or No
- **Computer Enclaves**	X	A	Values are Blacknet, FBINet, SCINet, and UNet
- **Organization Point of Contact**	X	A	
- **Documents**	X	A	On-boarding and separation documents
- **Task Force Type**	X	A	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Task Force Agency**	X	A, B	Detailee's agency
- **Task Forces**	X	A	Values include Counterintelligence Task Force, Joint Terrorism Task Force, Organized Crimes Task Force, etc.
- **Task Force Division**	X	A	
- **Task Schedule Type**	X	A	Values are Part Time and Full Time
- **Identity Management Request Status**	X	A	Values are Open, Closed or Discontinued
- **Visit Request**	X	A, B, C and D	Values are Approved and Denied
- **Work Mailing Address**	X	A	
- **SI start date, and credential expiriation date.**	X	C	
- **SI credential expiration date.**	X	C	

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

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

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify):					

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

Other (specify):

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Users and case-by-case recipients of information have a need to know security clearances and facility access permissions for FBI personnel and visitors.
DOJ Components	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.
Federal entities	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.
State, local, tribal gov't entities	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.
Public	X			Visitors have a need to know visitor security clearances and facility access permissions.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Visitors/visitor-sponsors have a need to know relevant security clearances and facility access permissions.
Private sector	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Foreign governments	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.
Foreign entities	X			Visitors/visitor-sponsors have a need to know visitor security clearances and facility access permissions.
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

It is not anticipated that Phoenix data will be released to the public under the circumstances contemplated by this question.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Notice for individuals who have been granted access but need to update their contact information is provided via a Privacy Act statement, which states:

> Phoenix collects your personal contact information, including your home address, phone number(s), and email address(es). Collection of this information is authorized by 5 U.S.C. § 301 and 44 U.S.C. § 3101. Providing this information is voluntary, and has no impact on your employment status. This information will be used to provide managers and security personnel with your contact information. Failure to provide this information may result in the inability of your supervisor or other members of the FBI to contact you in the event of an emergency.
>
> Your personal contact information will be treated in accordance with the following System of Records Notices (SORNs): Bureau Personnel Management System, FBI-008, 58 Fed. Reg. 51875 (October 5, 1993), as modified; Emergency Contact Systems for the Department of

Justice, DOJ-009, 69 Fed. Reg. 1762 (January 12, 2004), as modified; and General Personnel Records, OPM/GOVT-1, 77 Fed. Reg. 73694 (December 11, 2012), as modified. This information is being collected for internal purposes only, and it is not anticipated to be disseminated outside of the U.S. government. However, specific details as to the permissible routine uses of this information may be found in these SORNs.

Notice is also provided pursuant to the following system of records notices published in the Federal Register: *DOJ Insider Threat Program Records*, 82 Fed. Reg. 25812 (Jun. 5, 2017) amended by 82 Fed. Reg. 27872 (Jun. 19 2017); *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 Fed. Reg. 24147 (May 25, 2017); *Bureau Personnel Management System*, 58 Fed. Reg. 51875, amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); and *Security Access Control System*, 70 Fed. Reg. 7513, 516 (Feb. 14, 2005), amended by 82 Fed. Reg. 24147 (May 25, 2017).

These SORNs provide 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 applicable to this system provide additional notice about the ways in which information maintained by the FBI may be shared with other entities.

In addition, the DOJ Information Technology, Information Systems, and Network Activity & Access Records SORN, 86 Fed. Reg. 132 (July 14, 2021), is applicable to this system.

Lastly, HR Source, which provides employee identifiers to Phoenix, provides notice via its own Privacy Act statements and SORNs.[8]

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals may decline to provide information. However, refusal to provide information may result in the FBI's inability to provide the security clearances and facility accesses required for employment at the FBI or to access NATO clearance read-in materials.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

FBI contractors and detailees can access and update biographic information via the Phoenix self-

[8] The SORNs applicable to HR Source are *Bureau Personnel Management System*, 58 Fed. Reg. 51875, amended by 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017); *Emergency Contact Systems for the Department of Justice*, 69 Fed. Reg. 1762 (Jan.12, 2004), amended by 82 Fed. Reg. 2417 (May 25. 2017); *DOJ Information Technology, Information Systems, and Network Activity & Access Records*, 86 Fed. Reg. 132 (July 14, 2021); and *Correspondence Management Systems for the Department of Justice*, 66 Fed. Reg. 29992 (Jun. 4, 2001), amended by 66 Fed. Reg. 34743 (Jun. 29 2001), 67 Fed Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

service portal. FBI employees can access and update biographic information via the HR Source self-service portal. Inaccurate information reflected in the denial of physical access or security clearances can be amended by contacting SecD. Applicants and visitors cannot directly access or update their information, but can resolve errors or omissions through their FBI POC. Lastly, individuals may gain access to Phoenix information via the Freedom of Information Act, Privacy Act, or other legal process (e.g., legal discovery).

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO granted 8/30/2022; expires 5/9/2023 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no outstanding POAMs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:

<table>
<tr><td>X</td><td>This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:
<table>
<tr><td>Confidentiality</td><td>The system contains information that requires protection from unauthorized disclosure.</td><td>Moderate</td></tr>
<tr><td>Integrity</td><td>The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification.</td><td>Moderate</td></tr>
<tr><td>Availability</td><td>The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.</td><td>Moderate</td></tr>
</table></td></tr>
<tr><td>X</td><td>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
The EASP Information System Security Officer (ISSO) scans Phoenix monthly to ensure that the application is configured to meet the minimum Defense Information System Agency (DISA) and FISMA standards and is compliant with the most current Security Technical Implementation Guides (STIGs).</td></tr>
<tr><td>X</td><td>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:
Phoenix is audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. Audit logs are reviewed monthly by the EASP ISSO, using Kibana,[9] a data visualization tool. Users are subject to account suspension and referral to the Security Division (SecD) for further investigation.</td></tr>
<tr><td>X</td><td>Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.</td></tr>
<tr><td>X</td><td>Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:
Training on using the system is provided for new users and on-demand.</td></tr>
</table>

[9] Kibana is subject to review in separate privacy documentation as necessary.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The key privacy and security administrative, technical, or physical controls for minimizing privacy risks are as follows:

- Access to Phoenix is password-protected (via Active Directory). In addition, access to Phoenix is role-based. Not all users have access to all data.
- Physical Access to the server is limited to System Administrators, who must have valid security clearances and 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 controlled using Enterprise Security Assertion Markup Language (SAML) to support single sign-on user authentication and mitigate the potential for users to log into the system as another user.
- Phoenix is a networked-system accessible only via FBINet, a secure enclave; remote and mobile access is not available.
- Phoenix is manually audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. Audit logs are reviewed monthly by the EASP ISSO using Kibana. Inappropriate usage is subject to account suspension and referral to SecD for further investigation.
- User accounts are disabled immediately when personnel are no longer actively employed within the program or are found to be using information inappropriately.
- Vulnerability scans are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.
- Phoenix information is encrypted at rest and in transit using Advanced Encryption Standard (AES) 256-bit encryption and/or Secure Sockets Layer (SSL)/Transport Layer Security (TLS) tunnels.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The disposition of Phoenix information is described in the National Archives and Records Administration General Records Schedule 5.6, *Security Management Records*.

- Personal identification records and cards: "Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use." Id.
- Temporary and local facility identification and card access records: "Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance to to nearing expiration or not to exceed 6 months from time of issuance or when individual no

longer requires access, whichever is sooner, but longer retention is authorized if required for business use." Id.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

DOJ Insider Threat Program Records, 82 Fed. Reg. 25812 (Jun. 5, 2017) amended by 82 Fed. Reg. 27872 (Jun. 19 2017); *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 Fed. Reg. 24147 (May 25, 2017); *Bureau Personnel Management System*, 58 Fed. Reg. 51875, amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); and *Security Access Control System*, 70 Fed. Reg. 7513, 516 (Feb. 14, 2005), amended by 82 Fed. Reg. 24147 (May 25, 2017).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

The type, quantity, and sources of information collected and used by Phoenix are necessarily robust to allow the FBI to make responsible physical access and security clearance determinations for FBI personnel, visitors and applicants. Information is only shared as needed to facilitate information and facility accesses and determinations.

- The privacy risks associated with the collection and maintenance of Phoenix information are

inaccurate information, unauthorized access, and unauthorized disclosures.

- The privacy risks associated with the access and use of Phoenix information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of Phoenix information are the risks of unauthorized disclosures and loss of data.

The risk of inaccurate information is mitigated by the fact that biographic information is provided by the individual, either directly through the Phoenix self-service portal, or via HR Source (including the APPLY.FBIJOBS.GOV website for applicants). Inaccurate information reflected in the denial of physical access or security clearances can be amended by contacting SecD.

The risks of unauthorized access, unauthorized disclosures and loss of data are mitigated by the system, physical access, network-infrastructure and auditing controls, as described more specifically in Sections 6.1 and 6.2. These mitigations are in compliance with FIPS Publication 199.

Lastly, notice is provided by the Privacy Act statement and applicable SORNS, as described more specifically in Section 5.1.