# Federal Bureau of Investigation


**Privacy Impact Assessment**
for the
BICS Online (BOL) & BICS Online Transfer System (BOLTS)

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: June 17, 2021

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

# EXECUTIVE SUMMARY

The BICS Online (BOL)/BICS Online Transfer System (BOLTS) is a cross-domain information system used to manage the FBI's Security Division Background Investigation Contract Services Unit's (BICSU's) background investigations for federal employees and applicants. The system is comprised of two components: (1) BOL, an FBI Secret Enclave (FBINet) web-based application that tracks the investigation process and provides a data store for applicant background investigation information; and (2) BOLTS, an FBI unclassified network (UNet) outward facing web application that allows Special Investigators (SIs) with an Internet-capable device and a Law Enforcement Enterprise Portal (LEEP) account to electronically submit background investigation data to BOL. BOL/BOLTS replaces the manual delivery process of mailing work assignments via FedEx, submitting reports via Law Enforcement Online (LEO)[1] email, and faxing SI invoices.

This PIA is conducted pursuant to Section 208 of the E-Government Act of 2002, P.L. 107-347, which requires that agencies conduct PIAs on information technology systems that collect and maintain identifiable information regarding individuals. As changes are made to BOL/BOLTS operations and systems, this PIA will be appropriately reviewed and revised. This PIA will be published on FBI.gov.

## Section 1: Description of the Information System

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

The FBI is 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. BICSU Personnel Security Specialists (PSSs)[2] coordinate the background investigation process. BICSU utilizes contract SIs, who hold a Top Secret security clearance, to conduct background investigation interviews.

BOL is an FBINet web-based application that tracks the background investigation process and stores background investigation information. BOLTS is a UNet outward-facing web application that serves as a portal to the BOL.

Using BOLTS, SIs can electronically manage their workload (e.g., receive assignments, complete

[1] LEO provides electronic communications services for e-mail, data sharing, national alerts, analytical tools, applications, and enterprise services between the FBI and its mission partners at the local, state, tribal, and federal level for Sensitive but Unclassified/Controlled Unclassified Information. LEO is subject to separate privacy documentation.

[2] PSSs are FBI employees or contractors.

Personnel Security Interview reports (PSIs) and Reports of Investigation (ROIs),[3] submit invoices, provide assignment updates) from FBI-controlled on-line file storage accounts that can be accessed from workstations and laptops. Security Division is currently piloting changes to the document submission process associated with BOL/BOLTS to provide greater security to the information housed in the systems as required by the FBI Office of the Chief Information Officer.

Using BOL, BICSU PSSs review all applicant-related documents, including documents transmitted by SIs from BOLTS to BOL, and ensure that SI taskings are completed. BICSU PSSs generally do not conduct any interviews or perform any background checks.[4]

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

PSSs logon to BOL via a secure URL on FBINet. Users are authenticated using the FBINet Windows Active Directory (AD)[5] and single sign-on. BOL users can then coordinate all phases of the background investigation process such as receive leads, assign work, estimate work, approve work, obligate funding, review and process reports to/from Sentinel (the FBI's case management system), and review and process SI invoices to/from the Unified Financial Management System (UFMS) (the Department of Justice's (DOJ's) enterprise-wide financial and acquisition management system).

SIs must plug a BOLTS-specific encrypted thumb drive into their personal computer to connect and logon to BOLTS via a secure URL through the Criminal Justice Information Services (CJIS) Law Enforcement Enterprise Portal (LEEP). BOLTS users can then perform a variety of background investigation activities such as submitting reports and invoices, and downloading assignments and documents. SIs retain the information they collect as part of the background investigation process, as well as the information they download from and upload to BOLTS, on the same encrypted thumb drive that they must also use to log in to BOLTS. Although during the time the BOLTS-specific thumb drive is connected to the SI's personal computer, information transmitted from BOL through BOLTS can be viewed on that computer, once the thumb drive is removed from the SI's personal computer, none of the information that is on the thumb drive or that was transmitted through BOLTS either to or from BOL is retained in any way on the computer.

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

BOL/BOLTS and the related thumb drives contain applicant information, including academic, residential, achievement, performance, attendance, disciplinary, employment, criminal, financial, credit, publicly available social media, and personal and professional reference information.[6]

---

[3] PSIs document applicant interviews; ROIs generally document non-applicant interviews (e.g., references, employers, non-FBI applicants).
[4] PSSs may conduct interviews and background checks involving classified information.
[5] AD is a set of processes that authenticates and validates user access to FBINet. Thus BOL users do not need to re-enter logon credentials to specifically access BOL
[6] In limited instances, where extraordinarily sensitive background check-related information is involved (such as counterintelligence information, or confidential human source information), means other than BOLTS are used to transmit

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

Users are BICSU PSSs and SIs, and require approval from a BICS supervisor or program manager to obtain access to BOL or BOLTS. BICSU PSSs have access to all cases in both BOL and BOLTS. SIs only have access to BOLTS and their respective case portfolios.

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

SIs log into BOLTS and retrieve their respective work orders (list of interviews and/or investigative checks). Data can only be retrieved by work order number, which maps to an applicant Assignment Sheet (master applicant work order) in BOLTS. Data is also maintained on and retrieved by the SIs from the encrypted thumb drive that must be used to access BOLTS. Each SI maintains one such encrypted thumb drive that may maintain background check investigation information for up to approximately 30 case files at a time.

BICSU PSSs can access information in BOL by case number, work request number, work order number, and applicant name. BICSU PSSs do not log into BOLTS.

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

BICSU PSSs download the Lead Sheet (applicant name and Assignment Sheet), the applicant completed SF-86 (questionnaire for national security positions) and release forms[7] from Sentinel and upload these documents to BOL. The Lead Sheet leads are then parsed by BICSU PSSs into individual SI work orders based on the zip code of the interviewee. The candidate's SF-86, release forms and work orders are transmitted from the FBINet system, BOL, to the UNet system, BOLTS, through an encrypted cross domain solution, and finally from BOLTS to the thumb drive maintained by the SI.[8] The forms are deleted from BOLTS upon thumb drive download by the SI or within 24 hours, whichever occurs first. After 24 hours, any records not downloaded are deleted and must be requested again by the SI.[9]

The thumb drives onto which SIs download information are encrypted according to Federal Information Processing Standard (FIPS)140-2 requirements.[10] In fact, all information maintained in or

---

information from the SI to FBI secure data storage locations.

[7] The release forms authorize the SI to collect applicant information including current and historic academic, residential, achievement, performance, attendance, disciplinary, employment, criminal, financial, and credit information, and publicly available social media information.

[8] Cross domain transfer is effected by BOL sending a Hypertext Transfer Protocol Secure (HTTPS) request to BOLTS every 5 minutes through a scheduled command script. The HTTPS request queries BOLTS to see if there are any transactions waiting. BOLTS will send an HTTPS response, which is routed through the unclassified enclave firewall to the cross domain and content inspection software, to ensure that the appropriate file extensions are present and that the file does not contain any malicious data. The response is then routed through the classified enclave firewall for receipt by BOL.

[9] Assignments and documents that need to be requested are listed on the SI's home page.

[10] FIPS 140-2 can be accessed at https://csrc.nist.gov/publications/detail/fips/140/2/final.

transferred between BOL, BOLTS, and the associated thumb drives is encrypted at rest and in transit. The cross domain solution also includes a content inspection, so if a classification marking of "SECRET" exists anywhere in the document, the entire document will be rejected and not be transferred to BOLTS, and the lead will be addressed by a BICSU PSS. All business transactions that occur between BOL and BOLTS are secured to applicable NIST 800-122 recommendations and tracked for auditing purposes. Final applicant reports and all supporting documentation are uploaded to Sentinel.

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

BOL interfaces with UFMS (to process SI invoices), Sentinel (to retrieve Lead Sheets, SF-86 and release forms), and CJIS LEEP (for BOLTS' user authentication).

# 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 | x | Financial account | x |
| Taxpayer ID | x | Driver's license | x | Financial transaction | x |
| Employee ID | x | Passport | x | Patient ID | x |
| File/case ID | x | Credit card | x | | |
| Other identifying numbers (specify): Student ID | | | | | |

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

| **Work-related data** | | | | | |
|---|---|---|---|---|---|
| Occupation | x | Telephone number | x | Salary | x |
| Job title | x | Email address | x | Work history | x |
| Work address | x | Business associates | x | | |

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

| System admin/audit data | | | | | |
|---|---|---|---|---|---|
| User ID | x | Date/time of access | x | ID files accessed | x |
| IP address | | Queries run | | Contents of files | x |

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

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

| Government sources | | | | | |
|---|---|---|---|---|---|
| Within the Component | x | Other DOJ components | | Other federal entities | |
| State, local, tribal | | Foreign | | | |
| Explanation: Although SIs collect background check information from potentially all of these government sources, the information is compiled and contextualized by the individual SI within the component (FBI). | | | | | |

| Non-government sources | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, internet | | Private sector | |
| Commercial data brokers | | | | | |
| Explanation: Although SIs collect background check information from potentially all of these non-government sources, the information is compiled and contextualized by the individual SI, who is a government source. | | | | | |

## 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 to perform applicant background investigations pursuant to the Federal Investigative Standards (FIS) as promulgated by the Director of National Intelligence (DNI) and the Office of Personnel Management (OPM) from time to time. The privacy risks associated with the information collected are unauthorized access, breach, and misuse.

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

- User access is role-based. Not all users have access to all data.

- BOL/BOLTS is housed in an off-site data center. Physical access to the servers is limited to FBI System Administrators who receive privileged user training on an annual basis. Remote access for BOL users and application administrators is conducted from an FBINet workstation. The remote computer is located behind a firewall and runs anti-virus. Server administrative functions are via a Secure Shell (SSH) network connection.[11]

- Only system administrators can make configuration changes to the system. General users do not have permission to make configuration changes.

- The inherent system design of pulling data from UNet (BOLTS) to FBINet (BOL), and automatic purging of BOLTS data after 24 hours reduces the risk of unauthorized disclosure of, and access to, information.

- All access is password-protected.

- FBI personnel receive annual privacy and information assurance training.

- User groups are established by BOL/BOLTS management based on a defined need to know and a role that requires access to the data.

- User accounts are disabled immediately when BOL/BOLTS personnel are no longer actively employed by the program or are found to be using information inappropriately.

- SIs are required to save information to their FBI-approved thumb drives. When the thumb drive is connected to a PC, it mounts two drives: a secure volume and a CD drive. All files mounted within the CD drive are outside the logical boundary of the cryptographic module, as they cannot execute within the cryptographic boundary, cannot lead to a compromise of the module's security, and exist for storage only. However, the CD drive contents are read-only and protected by digital signature to prevent unauthorized modification and substitution, in accordance with FIPS 140-2, Level 2/3.

[11] SSH is a cryptographic network protocol that provides a secure channel for two computers to communicate with each other. Connection via SSH requires Multi-Factor Authentication (MFA) to access the BOL and BOLTS servers.

- The system has audit capabilities and is audited at a minimum every seven (7) days for the following events:
  1. Successful and unsuccessful attempts to access, modify, or delete security settings;
  2. Successful and unsuccessful logon attempts;
  3. Successful and unsuccessful changes and resets of passwords;
  4. Privileged activities or other system level access;
  5. Starting and ending time for user access to the system;
  6. Concurrent logons from different workstations;
  7. Successful and unsuccessful accesses to information system;
  8. All program initiations; and
  9. All direct access to the data, i.e., bypassing the BOL/BOLTS interface.

  The audit features are fully documented in the System Security Plan (SSP).

# Section 3: Purpose and Use of the System

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

| Purpose | | | |
|---|---|---|---|
| | For criminal law enforcement activities | | For civil enforcement activities |
| | For intelligence activities | X | For administrative matters |
| X | To conduct analysis concerning subjects of investigative or other interest (An applicant investigation is a form of investigation.) | | To promote information sharing initiatives |
| | To conduct analysis to identify previously unknown areas of note, concern, or pattern. | X | For administering human resources programs |
| | For litigation | | |

## 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.

BOL/BOLTS information collected, maintained and disseminated is necessary to vet federal job applicants in accordance with the FIS.

## 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. |
| X | Executive Order | E.O. 12333, Sec. 1.3(b)(20)(A);<br>E.O. 12333, Sec. 1.4(h);<br>E.O. 12333 Sec. 1.5(g);<br>E.O. 13388;<br>E.O. 13356. |
| | Federal Regulation | |
| X | Memorandum of Understanding/agreement<br>Executive Memorandum | FISS (Dec. 14, 2012). |
| | 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.)

BOL/BOLTS records are uploaded to Sentinel (or UFMS for invoice records) and are retained pursuant to the applicable retention schedule for those systems.

## 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: BOL

☐ **Low** ☐ **Moderate** ☑ **High**

PII Confidentiality Risk Level: BOLTS

☐ **Low** ☑ **Moderate** ☐ **High**

The potential impact of loss of confidentiality, integrity, or availability of BOL is HIGH because BOL contains PII for all current and historic background investigations since August, 2006. Thus, a loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to

organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The potential impact of loss of confidentiality, integrity, or availability of BOLTS is MODERATE because BOLTS only contains PII for individuals currently undergoing a background investigation, and only holds any documents containing such information for up to 24 hours. Thus, a loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss, or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- 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.**<br>**BOL: no remote access; BOLTS: remote access over encrypted channel.** |
| 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.**<br>BOL does not permit mobile access. The data transferred between BOL and BOLTS and thumb |

| | |
|---|---|
| | drives is encrypted. (BOLTS can be accessed by authorized users from any laptop or desktop with Internet access by using the BOLTS-specific thumb drive.) |

Audit controls

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

Identification and Authentication controls

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

Media controls

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

Data Confidentiality controls

| | |
|---|---|
| X | **Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used.** |
| X | **Protection of Information at Rest: data at rest encryption is employed on the primary and secondary storage device (e.g., hard drive or backup tape).** |

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 BOL/BOLTS include unauthorized access, loss of data, and inaccuracy of information. These risks are mitigated by the controls set forth in Section 2.3. In addition, BICSU enforces file and folder naming conventions to ensure that data is not uploaded to the incorrect applicant case folder.

# 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 | | | | |
| 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 unauthorized disclosures. These risks are mitigated by the controls set forth in Section 2.3. In addition, the risk of unauthorized disclosure is minimized by the fact that each SI only has access to his/her own cases, and disclosures are limited to intra-DOJ need to know disclosures and the routine uses described in the relevant System of Record Notices (SORNs) cited in Section 7.1.

## Section 5: Notice, Consent, and Redress

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

| | |
|---|---|
| X | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. |

| | | |
|---|---|---|
| X | Yes, notice is provided by other means. | Specify how: The SF-86 form that candidates are required to complete provides notice to the candidates. Non-candidate individuals interviewed in the course of a background investigation are provided verbal notice by the SI. |
| | No, notice is not provided. | Specify why not: |

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

| | | |
|---|---|---|
| X | Yes, individuals have the opportunity to decline to provide information. | Specify how: An individual can decline to provide information. However, such a declination will adversely impact the individual's eligibility for a national security position. Non-candidate individuals interviewed in the course of a background investigation can decline to provide information or request confidentiality. |
| | No, individuals do not have the opportunity to decline to provide information. | Specify why not: |

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

| | | |
|---|---|---|
| | 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: An individual can decline to consent to particular uses of the information. However, such a declination will adversely impact the individual's eligibility for a national security position. Non-candidate individuals interviewed in the course of a background investigation can decline to provide information or can request confidentiality. |

## 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 SORN cited 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.

In addition, form SF-86 provides notice of the information collection and uses to candidates, and the SIs provide such notice verbally to non-candidate individuals interviewed in the course of a background investigation.

# 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:<br><br>The System implements all applicable DOJ/FBI Core Security Controls for FISMA compliance, and, as set forth in Sections 2.3, 3.5 and 4.2, 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:<br><br>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 BOL users are authorized by Security Division Management to have access the system. Special Investigators must pass their background investigation, request (and be approved) for a LEEP account, and be granted access in BOL, which will then permit them to work cases in BOLTS.<br><br>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.<br><br>Privileged user accounts are disabled/deactivated when no longer needed, e.g., when an employee separates from the FBI or changes job description. | |
| X | The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation:<br>BOLTS ATO granted 9/8/2015; current extension is through 4/14/2021.<br>BOL ATO was granted 6/1/2014 (as part of the Enterprise Application Services Program (EASP)[12]); current ATO extension expires on 9/17/2021. | |
| X | Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:<br><br>The System inherits from the FBI ESOC the employment of automated mechanisms to integrate 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 7 days for indications of inappropriate or unusual activity and reports findings to designated FBI personnel with security roles, as described in Section 2.3. | |
| 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. |
| | N/A | Training specific to the system for authorized users outside of the component. |

[12] EASP is covered under separate privacy documentation.

| | | |
|---|---|---|
| | X | Other (specify): Annual Privacy Training |

### 6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Specific access and security controls to protect privacy and reduce the risk of unauthorized access and disclosure have been set forth in Sections 2.3, 3.5, and 4.2 above. Generally, however, to mitigate potential risks, BOL/BOLTS 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 Modernization 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.<br><br>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:<br>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); 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); 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). |
| | 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 BOL is retrievable by a candidate's name, case file number, work request number or work order number. Information in BOLTS is only retrievable by work order number.