# Federal Bureau of Investigation

# Privacy Impact Assessment
for the
# Enterprise Telecommunication Information System (ETIS)

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: [August 29, 2022]

***(May 2019 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 Criminal Justice Information Services (CJIS) Division's Enterprise Telecommunication Information System (ETIS) is the phone system for the CJIS Division. It facilitates communications inside and outside of the CJIS Division, links together all communications within the CJIS Division, and is used by all personnel located at the CJIS Division[1] as well as common areas and business entities within the CJIS Division, including the National Instant Criminal Background Check System (NICS), the National Threat Operations Center (NTOC),[2] the Biometric Services Section's (BSS) Customer Service Group (CSG), the Major Case Contact Center (MC3), and the CJIS help desk and switchboard operations. The ETIS maintains a log of all incoming and outgoing phone calls for the CJIS Division. For the business entities listed above, the ETIS also captures an audio recording of the phone call. Call recordings for outgoing calls for the business entities are only captured if the recording is manually initiated by the business entity. The call information is stored in a call log database with the audio and screen recordings of the call. ETIS also maintains a directory of all CJIS extensions and the name of the individual to whom the extension is assigned.

ETIS maintains logs of calls placed, as well as audio recordings of calls to the business entities for administrative purposes and to meet the business needs of the entities listed above. In addition, for the NICS Tier 1 (T1) call center, ETIS captures screen recordings for customer service representative (CSR) quality assurance reviews by NICS supervisors. NICS T1 screen recordings are maintained under the same 24-hour retention rule as NICS voice recordings. The ETIS system is comprised of the Avaya Public Branch Exchange (PBX) applications for the phone system and the Calabrio One software suite for the recording, speech analytics, and data transcription of calls. This Privacy Impact Assessment is being completed to discuss the privacy impact for maintaining caller identification information, the audio file recordings of telephone calls, and the screen recordings for the NICS T1 call center.

## 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.***

ETIS provides call delivery to all CJIS personnel and common areas and maintains a record of all telephonic communication into and out of the CJIS Division. ETIS logs all incoming and outgoing

---

[1] Personnel at the CJIS Division include FBI employees, contractors, and detailees as well as other federal agency liaisons stationed at the CJIS Division.

[2] NTOC also answers calls made to the FBI's Weapons of Mass Destruction Directorate (WMDD).

phone calls from CJIS. ETIS also provides call delivery to business entities at the CJIS Division. Typical call center call flow is as follows: Public callers place their calls from any type of telephone. The call is routed through the Public Switched Telephone Network (PSTN) to the appropriate call center. An Interactive Voice Response (IVR) system receives the incoming phone calls from the public and redirects the request to the appropriate business entity following a series of inquiry prompts-Intelligent Call Routing and Automated Call Distribution (ACD). Calls in the ACD queue are typically handled by the next available CSR/threat intake examiner (TIE). To meet the operational needs of the CJIS Division, the ETIS records all incoming phone calls made to the following business entities within CJIS as described below.

**National Instant Criminal Background Check System (NICS):**[3] NICS is a national name check system that queries available records in federal and state databases to determine if prospective purchasers of firearms are disqualified from receiving firearms. The NICS CSRs receive requests via phone calls from federal firearms licensees (FFL). FFLs calling NICS for firearm transactions provide their FFL license number and assigned codeword. Once the NICS CSR validates the FFL's information, the FFL provides personally identifiable information (PII) supplied by the firearm purchaser. This information includes the purchaser's name and date of birth and may also include the purchaser's social security number. The CSR initiates the background check with the firearm purchaser's information. If the NICS provides no negative hits, the CSR authorizes the FFL to proceed with the gun sale. Not all NICS checks are resolved during this telephone call because sometimes additional research is required. ETIS records all incoming calls to the NICS customer service centers. In addition, for the NICS T1 call center, the ETIS captures screen recordings of the CSR's computers. These calls and screen recordings are recorded for quality assurance purposes and are retained for 24 hours. During this 24-hour period, authorized NICS employees can access the call and screen recordings by logging in to specialized software within ETIS and retrieving the call by CSR name or agent identification number, automatic number identifier (ANI),[4] or date and time of the call.

**National Threat Operation Center (NTOC)**: NTOC protects the nation by serving as the primary communication channel through which the public provides information pertaining to federal crimes and threats to national security. By providing reliable, actionable, and high-value leads, NTOC assists FBI field offices and our law enforcement partners in ensuring public safety and national security. NTOC operates 24/7, 365 days per year, to examine and process information provided by the public for FBI investigative and intelligence purposes. NTOC receives telephonic information for all 56 FBI field offices, manages all electronic tips (E-Tips) submitted to the FBI through <tips.fbi.gov> and assesses potential threat information received through official FBI social media platforms. Information received by NTOC, with the exception of audio recordings, is stored in the Threat Intake Processing System (TIPS).[5] NTOC also serves as the MC3 for the FBI. The MC3 provides centralized case support of tip line information for FBI major cases and catastrophic events. The MC3 is utilized when a high volume of calls is expected and the field offices do not have sufficient staff to handle anticipated call volume. NTOC provides 24 hours a day, 7 days a week tip line support for

---

[3] NICS has separate privacy documentation and is covered by its own system of records notice, FBI-018.

[4] The ANI is the phone number from which the call initiates. If the call is transferred from a field office that does not pass the ANI, ETIS captures the main number of the field office. If the call is not initiated or transferred from a field office and the caller is not blocking his caller ID, ETIS captures the phone number from which the caller placed the phone call. ETIS only captures the ANI; ETIS does not capture the caller's name.

[5] TIPS has separate privacy documentation.

these cases and advertises a toll-free telephone number, <1-800-CALL-FBI>, for receiving the tips. For example, the MC3 may be activated when the FBI is looking for a high-profile fugitive or when a terrorist attack has occurred. Finally, NTOC processes calls for the Weapons of Mass Destruction Directorate (WMDD), which integrates and links all FBI counterterrorism, intelligence, counterintelligence, and scientific and technological components to accomplish the FBI's mission to prevent and respond to any terrorist threat or incident in the United States involving weapons of mass destruction (WMD) consisting of chemical, biological, or radiological material. NTOC answers telephone calls to the FBI WMDD toll-free telephone number.

NTOC TIEs answer all telephone calls to the FBI toll-free telephone number, the MC3, and the WMDD. TIEs collect information from callers and enter the information into TIPS. Callers may provide their name or other identifying information, or the call may be anonymous. Callers to NTOC may provide PII on other individuals about whom the caller is giving information to NTOC. ETIS records all incoming calls to NTOC for quality assurance, recordkeeping, and investigative purposes. Occasionally, TIEs make outbound calls for official purposes to obtain additional information from individuals who submitted information to NTOC.[6] When the TIE makes a return call for official purposes, the TIE records the phone call by using the recording controls tab within the Calabrio One user interface. This recording is necessary to adequately document any additional information the caller may provide. All outbound/return calls are initiated for follow-up purposes only as a result of a previously received phone call. ETIS maintains NTOC call recordings for five (5) years unless the call is marked by an authorized business entity representative to not be deleted. Calls recorded for NTOC may be sent to investigators following up on a lead from NTOC. To retrieve a call recording from ETIS, authorized NTOC employees log in to specialized software in ETIS and retrieve the call by the universal call identification (UCID) number associated with the call entry in TIPS. Call recordings can also be retrieved by TIE name or agent identification number, ANI, or date and time of the call. Once a call recording is pulled outside of the ETIS boundary, ETIS is not responsible for the integrity of the copy of the call recording. Authorized NTOC employees can also retrieve calls from ETIS directly from TIPS by clicking a player button in the TIPS' call entry. The player button pulls the call recording from ETIS for playback. ETIS also has the capability to transcribe an audio call recording and provide a keyword analysis using the Calabrio One software suite. This functionality is limited to only the NTOC business line. This "speech to text" capability creates a transcript of NTOC calls and is used for research and analytical purposes based on NTOC user guidelines. Access to the call transcripts is limited to approved NTOC personnel.

**Biometric Services Section Customer Service Group (BSS CSG):** The BSS CSG provides biometric identification services, including the processing of fingerprint submissions and criminal history records within the Next Generation Identification (NGI) system.[7] The BSS CSG receives telephone calls from the public and biometric information system users regarding updates on requests for criminal history records and fingerprint queries. Callers to the BSS CSG may provide PII on individuals to assist the CSR in locating records in the NGI system. The data provided by the callers to the BSS CSG may contain PII such as name, universal control number (UCN),[8] social security number, and date of birth. This information is not maintained within ETIS other than in the audio

[6] The practice of making outbound calls from NTOC for official purposes is rare and discouraged.
[7] NGI has separate privacy documentation.
[8] The UCN, also known as an FBI number, is a unique identification number assigned to each fingerprint submission to NGI.

recording of the call. All recorded calls to the BSS CSG are saved for 30 days for recordkeeping and quality assurance purposes. Authorized BSS CSG employees retrieve call recordings from ETIS by logging in to specialized software within ETIS. Call recordings can be retrieved by CSR name or agent identification number, ANI, or date and time of the call.

**The CJIS Help Desk and Switchboard Operations:** The CJIS help desk receives telephone calls, provides assistance to individuals utilizing CJIS Division services, and handles CJIS (all hours) technical support calls. The switchboard answers calls to the main CJIS phone number and directs callers to the appropriate individual or program. All inbound calls to the CJIS help desk and the switchboard are recorded and saved for quality assurance purposes for 30 days. Authorized help desk and switchboard employees retrieve call recordings from ETIS by logging in to specialized software within ETIS. Call recordings can be retrieved by CSR name or agent identification number, ANI, or date and time of the call.

Only the CJIS business entities listed above have the ability to record telephone calls. CJIS personnel at their desks or in common areas do not have call recording capabilities. All of the business entities that record calls notify callers in advance that their call may be recorded or monitored.

ETIS maintains a call log of all incoming and outgoing phone calls from the CJIS Division for recordkeeping purposes to track the CJIS Division's telephonic communications. The information can be used, if necessary, to recreate the CJIS Division's contacts with the public and with other governmental agencies. The internal phone directory supports the CJIS Division by providing employees with a tool through which employees can contact each other for official purposes. Audio recordings of incoming calls to the business entities' call centers and screen recordings of the NICS T1 call center are collected for quality assurance purposes to ensure that the CJIS Division is meeting customers' needs in a courteous and professional manner. In addition, by recording incoming calls to the business entities' call centers, the CJIS Division maintains a record of any threat made to a CSR/TIE via telephonic communication. This allows the CJIS Division to provide the recorded threat to appropriate security personnel and investigatory authorities. Likewise, by maintaining audio recordings of incoming phone calls to NTOC on tips, major crime contacts, and weapons of mass destruction calls, the CJIS Division is able, when necessary, to provide investigators with direct information for their investigations.

ETIS is contained within the CJIS Shared Enterprise Network (SEN).[9] Call and screen recordings and information are only resident on the CJIS SEN while in transit. Call log information is stored within ETIS. Call and screen recordings are stored encrypted on the permanent storage location within ETIS. The phone directory accessible to CJIS employees pulls information from the ETIS Communications Manager database. The phone directory provides the name and desk phone number of personnel at the CJIS Division. TIPS, a web interface designed and used by NTOC, connects to ETIS to perform functions as described above.

### *2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the*

[9] CJIS SEN has its own privacy documentation.

***information. (Check all that apply and include citations/references.)***

| | Authority | Citation/Reference |
|---|---|---|
| X | Statute | 5 U.S.C. § 301; 44 U.S.C. § 3101; 28 U.S.C. § 533 |
| | Executive Order | |
| | Federal Regulation | |
| | 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.***

ETIS maintains a log of all incoming and outgoing phone calls for the CJIS Division. When a phone call comes into CJIS, ETIS captures the date and time of the call, the ANI of the originating caller (when provided), the extension of the CJIS workstation answering the call as well as the name of the individual to whom the extension is assigned, and the length of the call. For outgoing calls, ETIS captures the extension of the CJIS workstation making the call as well as the name of the individual to whom the extension is assigned, the number called, the date and time of the call, and the duration of the call. For the business entities listed above, ETIS captures an audio recording of the incoming phone call. For the NICS T1 call center, ETIS also captures a screen recording of the CSR's computer. The call information is stored in a call log database with the audio and screen recording of the call. ETIS also maintains a directory of all CJIS extensions and the name of the individual to whom the extension is assigned. Call log information is maintained within ETIS. The call log information for the last 100 calls to and from a CJIS phone is saved locally on the phone. If employees are logged in to a call center, the call log information is maintained within ETIS. For contact information and administrative purposes, ETIS also maintains a phone directory containing CJIS personnel's names and the phone extensions assigned to each individual.

Information contained within ETIS call recordings for the various business entities differs based on the business entity for which the call is recorded. As discussed above, **NICS** receives calls from FFLs. FFLs calling NICS for firearm transactions provide their FFL license number and assigned codeword. Once the NICS CSR validates the FFL's information, the FFL provides PII supplied by the firearm purchaser. This information includes the purchaser's name and date of birth and may also include the purchaser's social security number.

TIEs from **NTOC** collect information from callers and enter the information into TIPS.

Callers may provide their name or other identifying information, or the call may be anonymous. Callers to NTOC may provide PII on other individuals about whom the caller is providing information to the FBI.

Callers to the **BSS CSG** may provide PII on individuals to assist the CSR in locating records in the NGI system. The data provided by the callers to the BSS CSG may contain PII such as name, UCN, social security number, and date of birth.

ETIS does not require social security numbers or other identifying information; however, individuals calling CJIS business entities may provide the information to CSR/TIEs during a call. Additional general personal data and work data may be provided by callers to CSR/TIEs during a call. Therefore, audio and screen recordings of calls captured by ETIS may contain social security numbers or other identifying information, general personal data, and work data. Within ETIS, audio call and screen recordings cannot be directly searched or retrieved by information provided verbally during a call. ETIS has the capability to transcribe an audio call recording and provide a keyword analysis using Calabrio One. This functionality is limited to only the NTOC business line. This "speech to text" capability creates transcripts of NTOC calls which are used for research and analytical purposes based on NTOC user guidelines. Only approved personnel have access to the transcripts. However, neither the audio recording nor the transcription can be retrieved from ETIS by information provided verbally during the call. Users retrieve audio and screen recordings and transcripts from ETIS via the Calabrio One user interface. The user interface only allows users to search for calls with metadata, including CSR/TIE name or agent identification number, date and time of call, or ANI (if available). NTOC users may also retrieve audio recordings and speech-to-text transcriptions by UCID or directly from the TIPS database.

The chart below indicates the types of information most likely to be contained in ETIS and its call and screen recordings; however, any type of information may be provided verbally if necessary.

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>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 | The ETIS call logs and phone directory contain names of personnel at the CJIS Division. Additional general personal data may be provided by callers to CSRs/TIEs, and therefore may be contained in recordings captured by the ETIS. However, in ETIS, call and screen recordings cannot be searched or retrieved by information provided verbally during a call. |
| **Date of birth or age** | X | A, B, C, and D | ETIS does not require dates of birth or other identifying information; however, individuals calling CJIS business entities may provide the information during the call. |
| **Place of birth** | | | |
| **Gender** | | | |
| **Race, ethnicity or citizenship** | | | |
| **Religion** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Social Security Number (full, last 4 digits or otherwise truncated)** | | | ETIS does not require SSNs or other identifying information; however, individuals calling CJIS business entities may provide the information during the call. |
| **Tax Identification Number (TIN)** | | | |
| **Driver's license** | | | |
| **Alien registration number** | | | |
| **Passport number** | | | |
| **Mother's maiden name** | | | |
| **Vehicle identifiers** | | | |
| **Personal mailing address** | | | |
| **Personal e-mail address** | | | |
| **Phone number** | X | A, B, C, and D | The ETIS call logs and phone directory contain telephone numbers and extensions assigned to CJIS personnel. In addition, ETIS captures the ANI of the incoming call. |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account information** | | | |
| **Applicant information** | | | |
| **Education records** | | | |
| **Military status or other information** | | | |
| **Employment status, history, or similar information** | | | |
| **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** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **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** | | | |
| **Procurement/contracting records** | | | |
| **Proprietary or business information** | | | |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |
| ***Biometric data:*** | | | |
| - **Photographs or photographic identifiers** | | | |
| - **Video containing biometric data** | | | |
| - **Fingerprints** | | | |
| - **Palm prints** | | | |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | x | A, B, C, and D | ETIS maintains audio recordings of phone calls for CJIS business entities; however, audio recordings are not searchable by voice signature. |
| - **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 | Files (not content of such) accessed/reviewed |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - **Content of files accessed/reviewed** | | | |
| - **Contents of files** | | | |
| **Other (please list the type of info and describe as completely as possible):** | x | A, B, C, and D | As discussed above, ETIS also captures a screen recording of NICS T1 CSR's computer screens. In addition, general personal data and work data may be provided by callers to CSR/TIEs during a call. Therefore, audio and screen recordings of calls captured by ETIS may contain social security numbers or other identifying information, general personal data, and work data. |

### *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 | | Hard copy: mail/fax | | Online | X |
| Phone | X | Email | | | |
| Other (specify): The phone directory includes names and phone extensions from personnel at the CJIS Division which is provided directly by the individual, via online service request, to receive a phone account. All call log information and information within call recordings is provided by telephone. | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Online | |
| 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): Information in the call recordings comes from individuals that call CJIS business entities which could include any government source. | | | | | |

| Non-government sources: | | | | | |
|---|---|---|---|---|---|
| Members of the public | X | Public media, Internet | | Private sector | X |
| Commercial data brokers | | | | | |
| Other (specify): Information in the call recordings comes from individuals that call CJIS business entities which could include any non-government source. NICS T1 call center screen recordings may capture information provided by FFLs. | | | | | |

## 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 | General users have direct access to their call logs and to the internal phone directories. Call recordings are accessed on a case-by-case basis by the business entity for which the call was recorded. See additional details in the narrative below. |
| DOJ Components | X | | | On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes. |
| Federal entities | X | | | On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes. |
| State, local, tribal gov't entities | X | | | On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes. |
| Public | | | | |

| 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.** |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | X | | | On a case-by-case basis, call recordings and other ETIS records may be shared for litigation purposes with appropriate legal process. |
| Private sector | | | | |
| Foreign governments | X | | | On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes. |
| Foreign entities | | | | |
| Other (specify): | | | | |

Direct access to information in ETIS is restricted to personnel at the CJIS Division with access to phone devices (desk phones for onsite work or soft phones[10] for remote work) or other ETIS system interfaces. ETIS user interfaces are only accessible from the CJIS Unclassified Network (CJIS UNet) by authorized ETIS users. Access controls for users are defined using roles based on the users' job functions and users' status which restricts access to only necessary system functions. General users include all personnel at the CJIS Division who are not logged in to a call center. General users have access to the phones at their workstation. Through the phone, general users can access the internal phone directory and the call log for their assigned extension. A user's call log retains a record of the last 100 calls to or from the extension. The call log provides the name of the individual calling the extension (if the individual is an internal user), the number from which the call originated (if the number is not blocked), the time and date of the call, and the length of the call. From the call log, general users can add individuals as contacts and call individuals. General users have the ability to clear the call log from their phone; however, the call log remains within ETIS.

Privileged users of ETIS include system administrators, application administrators, and system security administrators. Each privileged user type has different access to the information within ETIS:

**System administrators** administer ETIS and have the ability to troubleshoot the system, restart servers and services, and implement both environmental and functional system changes. System Administrators have access to the call logs and phone directories within ETIS.

**Application administrators** support the multiple application-level services including over a dozen key applications to maintain ETIS. A few select application administrators control, access, and

[10] Softphone software is a user-friendly interface that functions much the same way a regular phone would. It can be installed on a piece of equipment, such as a desktop or laptop. It allows the user to place and receive calls without requiring an actual physical phone.

make decisions related to implementation and management of the call and screen recording services. Application administrators monitor, troubleshoot, and assist business entities with accessing call and screen recordings and using ETIS' specialized software.

**Network administrators** have the ability to configure the network appliances and firewalls necessary for ETIS to function.

**Database administrators** maintain any back-end databases required to support ETIS.

**System security administrators (SSAs)** have primary responsibility for administering system security functions, managing user IDs and user accounts, and performing monitoring of security audit records. SSAs and the Information System Security Officer (ISSO) review security audit records including operating system and application logs at least weekly using various searches, reports, dashboards, and alerts. SSAs work closely with system administrators to maintain the system and to monitor system changes and user activity.

Call and screen recordings may be accessed by authorized privileged users and authorized users from the business entities based on different tiered levels of security access controls which are controlled by the business entity to which the call was directed. A business entity cannot see another's business entity's call recordings at the end-user level. For example, calls recorded for NTOC cannot be viewed by the BSS CSG. To access a call or screen recording, a designated authorized user within a business entity logs in to specialized software within ETIS. The specialized software allows authorized users to access the calls for their business entity. Users can search for call and screen recordings by CSR/TIE name or agent identification number, date and time of call, or ANI (if available). For calls into the NTOC, call recordings are also searchable by the UCID. The specialized software allows authorized users to listen to the call recording. ETIS software also allows business entities to review a small subset of recorded calls for quality purposes. NTOC can also retrieve call recordings directly from TIPS by clicking the player button. The player button pulls the call recording from ETIS for playback. If necessary for the business entity, the authorized user can download the call for further use consistent with the business entity's needs. Once downloaded, the call recording leaves ETIS and is controlled by the business entity's established processes for handling call recording information.

Call log information in ETIS can be retrieved by any data element in the call log. General users can search the ETIS phone directory on their desk phone by first and last name. Information within the phone directory is retrieved by first or last name. Information in personal call logs is maintained in chronological order. Information in the master call log database can be retrieved by date of call, time of call, ANI, or CJIS employee name or phone extension. Call and screen recordings are retrieved by CSR name or agent identification number, date and time of call, or ANI (if available). For calls into NTOC, call recordings and transcripts can also be retrieved by UCID.

ETIS audit logs can be retrieved by any data field in the log, but are most often retrieved by the following two fields: hostname or IP address for information specific to a server or system; user account ID for information of who or what is accessing the server or application.

### *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.***

Information from ETIS will not be released for open data purposes or for research or statistical analysis purposes. ETIS does not include specific capabilities for information sharing. Access to information in the system is restricted to personnel at the CJIS Division with access to phone devices (desk phones for onsite work or soft phones for remote work) or other ETIS system interfaces. ETIS user interfaces are only accessible from CJIS UNet by authorized ETIS users. CJIS UNet requires two-factor authentication for access. Call and screen recordings can be accessed only by authorized personnel from the business entities and ETIS system administrators. The majority of call and screen recordings are not extracted from the ETIS where they are encrypted at rest. For those call recordings that are downloaded for business entity purposes, the recordings may be shared within the FBI. For investigative purposes, NTOC may share call recordings with FBI field offices or other agencies with the authority and jurisdiction to investigate the matters reported within the call recording. When specific call recordings are extracted from ETIS, the business entities' established processes are used to control the handling of the extracted call recordings. Call recordings are only shared with and disclosed to those individuals or entities with a need to know in order to perform their authorized investigatory responsibilities.

## 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.***

ETIS collects minimal information in its call logs. For incoming calls, the ANI, if available, is collected which could possibly be traced back to a specific individual. For internal calls, only personnel's names and their extensions appear in the internal phone directory. All callers routed to a business entity for which calls are recorded hear an automated message informing them that the call will be monitored or recorded. Callers who do not wish to have the call recorded have the opportunity to hang up. Moreover, callers control what information they provide during a call. The minimal information maintained in the call logs is kept for administrative and record keeping purposes. This privacy documentation and the System of Records Notices listed in Section 7 provide notice to the public on how the FBI may use information voluntarily provided to the FBI through telephone calls.

***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.***

All incoming calls to the CJIS Division are voluntarily made. For the business entities for which calls are recorded, all callers are informed via an automated message that the call may be monitored or recorded. By continuing the call after being notified of the recording, callers are implicitly providing consent for the recording; however, the specific uses of information depend on the type of call and the needs of the FBI. Upon hearing the notification, the caller has the opportunity to

hang up. Callers control what information they provide to the CJIS Division during a call.

***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.***

Individuals may request access to their records by following the guidance provided on the FBI's website at https://www.fbi.gov/services/records-management/foipa. A request for access to a record from this system of records must be submitted in writing and comply with 28 Code of Federal Regulations (CFR) part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records. The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

## 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):** 10/01//2020<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**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:**<br><br>All the security controls relevant to the ETIS System using National Institute of Standards and Technology Special Publication (NIST SP) 800-37 and FBI OCIO policies have been reviewed and are continuously monitored in RiskVision. |

| | |
|---|---|
| | **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:** |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ETIS logically resides within the CJIS SEN environments and assumes a defense in depth architecture enforced from SEN. The CJIS employs security monitoring tools as defined by FBI policy. Monitoring tools employ mechanisms for alerting of anomalous behavior or indicators of attack. The CJIS Network Operations Center and Security Operations Center actively perform traffic analysis and monitor alerts to support detection.<br><br>ETIS is required to perform a formal ATO Security Assessment and Authorization derived from the tailored security requirements based on Federal Information Processing Standards 199 Categorization. This assessment requires that all applicable controls are addressed to ensure operational compliance within applicable NIST 800-53 REV4 and FBI policy. |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** SSAs and the ISSO review security audit records including operating system and application logs at least weekly using various Splunk searches, reports, dashboards and alerts. Log monitoring occurs daily during the week. Events are monitored 24/7 by the SSAs and the operations team. SSAs work closely with system administrators to maintain the system and monitor system changes and user activity. |
| X | **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**. |
| X | **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:** Privileged users are required to take annual training on contingency planning, incident response, data spill management, and information security. General FBI users are required to annually take information security training. All users must abide by the FBI Rules of Behavior. |

***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?***

Access to PII within the call logs and phone directory is restricted to personnel at the CJIS Division with direct access to phone devices or other restricted ETIS system interfaces. Access to information saved on phone devices is restricted to personnel at the CJIS Division with access to phone devices (desk phones for onsite work or soft phones for remote work) or other ETIS system interfaces. ETIS user interfaces are only accessible from CJIS UNet by authorized ETIS users. CJIS UNet requires two-factor authentication for access. Access to ETIS user interfaces requires an additional layer of authentication. Access controls for general users are defined using roles based on the user's job function that restrict access to only necessary system functions. Most ETIS network

communications are encrypted to protect sensitive data in transmission.

The greatest risk to privacy comes from the potential misuse or loss of PII disclosed by callers and captured during the call and screen recordings for CJIS business entities. As discussed above, the call and screen recordings are only accessible from the FBI CJIS UNet through specialized software within ETIS or from TIPS. CJIS UNet workstations, ETIS, and TIPS require two-factor authentication for access. Only specific CJIS UNet users are granted access to the workstations that have access to ETIS. Further, access to the call and screen recordings is provided via web interfaces accessible via ETIS that require another layer of authentication. Access to the call recording web interface is restricted to authorized personnel and ETIS system administrators. ETIS call and screen recordings are encrypted at rest. In the limited instances when a business entity needs to download a call recording for a business need, the call recordings are only shared with and disclosed to those individuals or entities with a need to know the information in the call recordings to perform their authorized investigatory or security responsibilities.

***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.)***

ETIS call recordings are retained as required for the type of call center call. In accordance with legal requirements, call and screen recordings for NICS are only retained for 24 hours and then purged. Call recordings for NTOC are maintained within ETIS for 5 years. Call recordings for the BSS CSG, the CJIS help desk, and switchboard operations are maintained for 30 days. General users' personal call logs retain the last 100 calls to or from the users' desk phone. General users can delete their personal call logs at any time. Call logs maintained within ETIS are retained within ETIS for 13 months and can be retrieved from backup storage for an additional year.

## 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:***

Depending on what type of PII is involved, several different DOJ SORNs may be applicable including: *Correspondence Management Systems for the Department of Justice*, **DOJ-003**, 66 *Federal Register* (FR) 29992 (June 4, 2001) as amended at 66 FR 34743 (June 29, 2001), 67 FR 65598 (Oct. 25, 2002), and 82 FR 24147 (May 25, 2017); *Employee Directory Systems for the Department of Justice*, **DOJ-014**, 74 FR 57194 (Nov. 4, 2009) as amended at 82 FR 24151, 153 (May 25, 2017); *The FBI Central Records System*, **DOJ/FBI-002**, 63 FR 8659 (Feb. 20, 1998) as amended at 66 FR 8425 (Jan. 31, 2001), 66 FR 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017); *The Next Generation Identification (NGI) System*, **DOJ/FBI-009**, 81 FR 27283 (May 5, 2016) as amended at 82 FR 24151,

156 (May 25, 2017); *National Instant Criminal Background Check System (NICS),* **DOJ/FBI-018**, 63 FR 65223 (Nov. 25, 1998) as amended at 65 FR 78190 (Dec. 14, 2000), 66 FR 6676 (Jan. 22, 2001), 66 FR 8425 (Jan. 31, 2001), 66 FR 12959 (Mar. 1, 2001), and 82 FR 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.***

Three types of information are retained in ETIS: a phone directory of personnel at the CJIS Division, call information associated to these individuals, and call and screen recordings capture for CJIS business entities as defined by each business entity's requirements. All information collected by ETIS presents risks to privacy concerning the accuracy of information maintained in the system. In order to mitigate risks created by inaccurate information, ETIS limits searchable data fields to the minimum amount of information necessary to properly log the call and identify points of contact for further investigation.

Information captured from the phone directory on personnel at the CJIS Division includes the name of the individual and the extension number ETIS assigns to the individual. This information is collected based on information that may be vetted by the individual prior to its inclusion in the phone directory. Because ETIS generates call logs based on the assigned extension, there is a risk that the CJIS personnel identified in the call logs may not be the individual who was actually on the call. Identification of the individual can be verified through direct contact with the individual.

Information concerning outside individuals falls into two subcategories: data that is automatically collected, such as the ANI (if available), and the content of the audio recordings. If the individual is calling from a number registered to him- or herself, the ANI could link back to the outside individual if further research is performed outside ETIS. Information concerning the owner of the ANI is not captured in ETIS, which limits the risk that ETIS records will misidentify an individual. Information provided throughout the course of the conversation about the outside individual is collected directly from the subject individual, which reduces the risk that information will be incorrect. There is a risk that information provided by the outside individual about others could be incorrect. However, none of the information provided throughout the course of the call is content searchable within ETIS, and call and screen recordings are kept for a limited amount of time unless deemed

relevant to an investigation and transferred to an outside system.

Because ETIS maintains PII in its call logs, call directory, and call and screen recordings, there is a risk that the PII could be improperly accessed, misused, or lost. To mitigate these risks, only minimal PII (personnel names and telephone extensions) is accessible to general users of the ETIS. More extensive PII data is stored within ETIS call and screen recordings, but the content of these recordings is not searchable by personal identifier. The recordings are only accessible from the CJIS UNet, specialized software within ETIS, and (for calls to NTOC) through TIPS. CJIS UNet workstations and access to ETIS and TIPS require two-factor authentication for access. Only specific CJIS UNet users are granted access to the workstations that have access to ETIS. Further, access to the recordings is provided via web interfaces accessible via specialized software that requires another layer of authentication. Access to the recording web interface is restricted to authorized personnel and ETIS system administrators. All FBI employees and contractors with access to ETIS are required to maintain an active, adjudicated security clearance. Also, all personnel are required to undergo annual privacy and information security training.