Federal Bureau of Investigation

Privacy Impact Assessment
for the
Threat Intake Processing System (TIPS)

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: [December 2, 2020]

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

EXECUTIVE SUMMARY

The Federal Bureau of Investigation (FBI) National Threat Operations Center (NTOC) provides the public 24 hours a day, 7 days a week access to submit information to the FBI via commonly used communication channels. NTOC receives, prioritizes, and processes actionable information. NTOC strives to provide reliable, actionable, and high-value leads to assist FBI field offices in ensuring public safety and national security. NTOC receives information verbally over the phone and also receives electronic information (E-Tips) that is submitted by the public to the FBI through a web form, interactions with the FBI's official social media sites, or via email. Professionally trained staff, supervised by special agents, answer telephone calls, process E-Tips, and document all relevant information in the Threat Intake Processing System (TIPS). This central operations center permits the FBI to respond more effectively to the wide variety of calls and E-Tips received from the public and ensure that they are all reviewed and routed for investigation as appropriate. This privacy impact assessment is being completed to assess the privacy risks associated with maintaining information in, and sharing information from, TIPS.

Section 1: Description of the Information System

(a) The Purpose of the National Threat Operations Center (NTOC)

The FBI's NTOC serves as a central intake point in the FBI for the general public and other government agencies to provide information about potential or ongoing crimes, threats to life (TTL),[1] and national security threats. The NTOC's threat intake examiners (TIEs) process telephonic information and E-Tips by completing preliminary research and analysis on the information received and documenting relevant information in TIPS. The NTOC TIEs, in collaboration with an NTOC supervisor, make a determination on the threat level associated with the information to determine if immediate action is required or if the information should be disseminated in the normal course of business. Prior to dissemination, TIEs build subject profiles, and then refer the information to the appropriate FBI entity or other appropriate federal, state, local and/or tribal partners. NTOC works 24 hours a day, 7 days a week, 365 days a year and strives to provide reliable, actionable, and high-value information to FBI field offices and other partner agencies.

NTOC is a key component in the FBI's initiative to provide timely and direct notification of every TTL received by NTOC to the appropriate FBI field office operations center. When necessary, NTOC provides direct communication to state, local, and tribal partners on emergent TTL matters to ensure a timely response. The NTOC TIEs receive, analyze, and disseminate information pertaining to potential and actual emergencies and national security situations through the use of probing questions to determine the existence of a threat or crime. The TIEs are supervised by supervisory special agents, office services supervisors, and lead TIEs who are trained to triage threats to national security and emergency situations such as cyber threats, bomb threats, active shooter incidents, and hostage

[1] Threat to life (TTL) tips are defined as tips containing information about a threat to human life, serious bodily injury, or significant violent action.

situations; take appropriate actions; and follow guidelines and policies to ensure timely communication of actionable leads.

In addition to acting as the national operations center, NTOC serves as the Major Case Contact Center (MC3) for the FBI. The purpose of the MC3 is to provide 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 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.

(b) How the NTOC Achieves its Purpose

The NTOC TIEs answer telephone calls, process E-Tips, and document pertinent information in TIPS. All calls and E-Tips received by NTOC are logged in TIPS via an internal-only, web-based application, including those that are unintelligible or inaudible or are referred to other government jurisdictions/services or other tip lines. TIEs also conduct research and perform database queries using information provided during the call or in the E-Tip submission. This research is conducted in both classified and unclassified systems and may include researching open source information and publicly available social media. TIEs perform this research to corroborate the information provided, add additional relevant information, determine if there is a connection to an existing FBI case and link previous related transitions. TIEs write a synopsis of the information provided by the caller and the pertinent results from their database queries and make notations regarding the frequency and nature of the calls and E-Tips, including those received by individuals who make frequent and/or baseless submissions or postings. TIEs attach screenshots of relevant information found during open source research and other documentation on the NTOC's handling of a tip.

For those calls and E-Tips which report potential violations of criminal law and/or threats to national security, the TIE electronically documents information in TIPS and directly submits the information from TIPS through the FBI's eGuardian[2] system to be migrated to the FBI's internal Guardian[3] system on a complaint form. These forms are sent electronically via Guardian to the appropriate field office for further review and investigatory actions. When information is located while dispositioning a lead, the TIE may forward the information within the FBI or to other agencies within the area of responsibility (AOR). This information may be forwarded through the eGuardian system, an email to the appropriate agency, or a direct submission by the TIE to the appropriate agency's electronic tip form. For example, if information is received by NTOC and deemed to be of local jurisdiction, NTOC may provide the tip information, via eGuardian or direct sharing, to the appropriate

[2] eGuardian is a secure, unclassified system whereby the FBI and its law enforcement partners can coordinate information sharing and reporting on terrorism threats and suspicious activity. The application works in tandem with Guardian, allowing information to be immediately available to all authorized users. eGuardian has separate privacy documentation.
[3] Guardian is the FBI's enterprise threat intake and assessment management application. Guardian has separate privacy documentation.

fusion center[4] or local law enforcement entity for dissemination; threats against the President may be forwarded to the United States Secret Service (USSS); and information regarding child exploitation that does not rise to the level of a federal crime may be sent to the National Center for Missing or Exploited Children (NCMEC).

(c) Information in TIPS

TIPS stores information concerning the identity of the caller, such as name, telephone number, address, date of birth, and foreign language spoken, if applicable. It also includes information related to the nature of the complaint, such as identifying information regarding the alleged subject(s) and/or possible victim(s). Audio recordings of each call are maintained within the Enterprise Telecommunications Infrastructure System (ETIS)[5] and can be retrieved by the FBI for review. A transcription of the call, generated by speech-to-text software, is also included in the TIPS transaction. TIPS also stores information on E-Tips that are submitted by the public to the FBI through a website <tips.fbi.gov>, interactions with an official FBI social media site which are forwarded to TIPS, or threat information from private companies. E-Tips may include the tipster's name, telephone number, email address, username, street address, and/or internet protocol (IP) address. E-Tips may also include relevant attachments such as screen shots of threatening social media posts, photos, videos, or text files.

TIEs also search internal FBI systems regarding callers, victims, and subjects to determine if an open or related FBI case already exists or if the FBI has additional information on an individual (such as criminal history record information); and external sources of information publicly available on the internet (e.g. publicly available social media information) to assess the validity of allegations of threats or criminal conduct. These searches and information found are documented in TIPS. Screenshots of relevant information found on publicly available social media may also be included in TIPS. TIEs also document each disposition and may provide user notes including details on why the TIE made the disposition decision. TIEs may include attachments to document steps NTOC took during the disposition process. Documents may include requests sent to private companies for pertinent information and any voluntarily provided response. If the information is reviewed by a supervisor or for quality management purposes, user notes may be manually entered to provide their observations or disposition decision.

TIPS may also contain disposition information. The records in TIPS contain basic biographic and complaint information, information on the disposition of the lead (e.g. sent through eGuardian/Guardian to a field office; documented for domain awareness; emailed to the field office; sent via Crisis Intake; emailed to the USSS; referred to NCMEC; referred to other federal, state, local, or tribal agency), limited information about databases checked, and information found during internal database checks and from external sources, including screenshots of relevant information. TIPS contains a link to the eGuardian form but not the form itself. More comprehensive Guardian reports are

[4] Fusion Centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, territorial; and private sector partners.
[5] The ETIS has separate privacy documentation.

not maintained in TIPS.

TIPS also contains information regarding quality assurance, which is segregated and only available to authorized users based on their designated user role. This information consists of the completed TIPS transaction being reviewed, to include any accompanied attachments to the transaction, questions for the quality assurance reviewer to answer during their assessment, and notes/determinations made by the quality assurance reviewer.

TIPS maintains a list of individuals who have submitted baseless information which is identified as harassing or excessive. The list contains identifiers for each individual (such as first, middle, and last name, date of birth, telephone number, address, IP address, and email address). When an individual is added to this list, notification is sent to the FBI field office whose AOR most likely covers the individual's identified location. In addition, if a telephone number is blocked from calling NTOC and a current address can be identified for the individual, NTOC attempts to send notification either to the subscriber of the telephone number or the actual caller.

TIPS also includes information on the TIPS users. This information includes the user's name, email address, username, designated user role in TIPS, and the NTOC identification number. In addition, an individual's associated FBI field office or division is captured for users who access TIPS via the Law Enforcement Enterprise Portal (LEEP).[6] Audit logs are maintained on each individual user to provide record of the user's actions, such as what the user searched and which transactions were opened, closed, viewed, or edited by the user.

(d) Access to TIPS Data

The National Threat Operations Section (NTOS) controls direct access to TIPS. Direct access to TIPS is available only to FBI personnel (i.e., employees, contractors, and task force officers). To receive access to TIPS, FBI personnel must contact the designated NTOS points of contact who validate access criteria was met. Upon notification an employee has left NTOS and is no longer processing NTOS work, the designated NTOS points of contact terminate the user's access. The access control list for TIPS is reviewed when employees join or leave NTOS. FBI personnel who support NTOS have full access to TIPS to process and document incoming information as appropriate. FBI personnel who work outside of NTOS or who do not support NTOS are provided with read-only access to TIPS via LEEP. Read-only access is controlled via LEEP identity providers. Only a user with an fbi.gov unclassified network identity can access TIPS Read-Only. This read-only access allows the FBI personnel to search TIPS for information pertinent to their AOR, intelligence collection, or ongoing investigation. Information which is identified by NTOC as sensitive in nature and marked as restricted is not available to all TIPS users. Restricted information is only viewable by individuals who

[6] The LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems and ensuring that only authenticated users have access to those systems and services. LEEP has separate privacy documentation.

have the corresponding TIPS user role, which allows a user the ability to designate and view the restricted files. As stated above, tips that report potential violations of criminal law and/or threats to national security are documented and, based upon the provided information, sent to the appropriate FBI field office for review. Information from TIPS may be shared within the FBI or with other federal, state, local, or tribal agencies if the information is pertinent to their AOR. For example, if TTL information is received by NTOC and deemed to be of local jurisdiction, NTOC may provide the information, via eGuardian or direct sharing, to the appropriate fusion center or local law enforcement entity for dissemination. To ensure the local entity is notified timely, NTOC may also contact the local entity via telephone to advise them of the impending information. In addition, information regarding crimes against children that does not rise to the level of a federal crime may be sent to NCMEC.

External agencies do not have access to TIPS; rather, information is passed to the agency through interoperable systems, emails, or telephone calls by a TIE or an FBI field office. In certain circumstances, TIEs may directly email information from TIPS to another portion of the FBI or another agency. For example, information regarding threats against the President can be emailed to the USSS via an email template within TIPS. On a limited scale, TIEs may encounter a call from an individual expressing suicidal ideation. In these instances, NTOC may provide the caller with the National Suicide Hotline phone number. NTOC will also attempt to obtain the caller's location in an effort to then notify their local law enforcement. On a case-by-case basis, NTOC may share limited information from TIPS with private companies to help identify or locate the subject of a threatening lead or to help determine where to send the information. This may include providing information and usernames to companies to determine a subject's identity; providing IP addresses to private companies to receive location information on where the IP address is being used; or providing addresses or telephone numbers to companies to determine the appropriate state, local, or tribal law enforcement agency or 9-1-1 center to which to route information.

When NTOC serves in the MC3 capacity, information may also be sent via a Crisis Intake form to the FBI's crisis management module within Sentinel.[7] Although FBI personnel have read-only access via LEEP, NTOC may still be contacted by an FBI field office and asked to search TIPS and provide information, including call recordings, to FBI personnel to assist with investigations. For example, if requested for an FBI investigative purpose, NTOC staff will search TIPS and inform an inquiring FBI employee if an individual has previously submitted information or was the subject of a previous TIPS entry.

To ensure the FBI connects TIPS data with existing FBI assessments, investigations, cases, and information, search criteria from TIPS data will be sent to other FBI systems, such as the National Crime Information Center, to search for matching records. Automated searching of other FBI systems may include the transmission of TIPS search criteria to FBI systems via a machine-to-machine connection. NTOC will define search criteria (e.g. name, date of birth, telephone number, address, social security number, etc.), and the other FBI systems will execute the searches and consolidate the

[7] Sentinel is the FBI's internal case management system that contains all investigative files. Sentinel has separate privacy documentation.

search results for NTOC evaluation. Search results from unclassified systems will be displayed in TIPS. TIEs will review the search results for relevancy to the TIPS' entry. Relevant search results will be saved in TIPS. Any search results not deemed relevant to the TIPS' entry will not be saved in TIPS. For searches of classified systems, the systems will only provide an indication (yes/no) of whether a search produced any results; the actual search results are not sent to TIPS.

Only limited personnel have access to the TIPS audit logs. The TIPS audit logs are available to TIPS system administrators as well as TIPS users who are granted the appropriate permissions from NTOS. The audit logs are available via TIPS and access is controlled by permissions granted from designated points of contact within NTOS. IT personnel access the audit logs to troubleshoot issues. NTOS personnel use the TIPS audit logs to track the history of processed tips and create timelines of TIPS transaction when needed.

(e) Retrieval of Information from TIPS

Authorized personnel retrieve information from TIPS using biographic data to search the database from the web-based user interface. The TIPS entries can be searched and retrieved by personal identifiers (e.g. name, date of birth) or any keyword. Audio recordings of calls stored in ETIS can be retrieved by the FBI staff using the universal call identification number (UCID) associated with the TIPS entry or by clicking on the call recording button in the TIPS entry associated with the call.

The TIPS Read-Only access will not give authorized staff (FBI field personnel, task force officers, and contractors) access to audio recordings at this time. Field personnel will be granted access to actionable and non-actionable written synopses of TIPS entries, both electronic and telephonic. LEEP will act as the portal or gateway into TIPS. Once LEEP authenticates the field personnel user identity, they will have Read-Only access to the TIPS holdings, which means that field personnel will be able to search, retrieve, and view the TIPS data, but they will not be able to change the TIPS data or create or delete the TIPS entries. The TIPS Read-Only application can be searched and retrieved by personal identifiers (e.g. name, date of birth), any keyword, or field office AOR.

A list of the TIPS users and their information (e.g. name, email address, username, designated user role in TIPS, and the NTOC identification number) can be retrieved directly from TIPS by individuals with administrative access in TIPS. Administrative users can view audit log transactions on a specific tip transaction in TIPS through the use of administrative controls. Also, audit log information detailing all actions a user performs in TIPS can be obtained from the system's report server. These reports provide a record of the user's actions, such as what the user searched and which transaction was opened, closed, viewed, or edited by the user. Criminal Justice Information Services Unclassified Network (CJIS UNet)[8] System Security Administrator (SSA) and Information System Security Officer (ISSO) review TIPS audit logs weekly.

[8] The CJIS UNet is an unclassified FBI system. CJIS UNet has separate privacy documentation.

(f) Transmitting Information to and from TIPS

When a call is received by NTOC, TIPS automatically populates entry points in the database by pulling the number from which the call is placed, if available, from ETIS. The TIE answers the call and manually enters all additional information. This additional information includes the caller's information; a synopsis of what was reported on the call including information about subjects, victims, and witnesses;[9] results from database searches; a disposition of the call; and user notes which provide details on why the TIE made the disposition decision for the lead. The TIEs may also attach documentation of additional steps taking while dispositioning a lead. In addition, if a lead is reviewed by a supervisor or for quality management purposes, user notes may be manually entered to provide information regarding their observations or disposition decision. A transcription of the call generated by speech-to-text software is also included in the TIPS transaction. The public can also submit E-Tips to the FBI through the <tips.fbi.gov> webpage or other official FBI channels. E-Tip submissions may include attachments. E-Tips are emailed to TIPS, which is programmed to ingest these emails and convert them to TIPS entries for processing.

Some information in TIPS may be automatically populated from application programming interfaces (APIs) with external companies. For example, to find the location of a subject, TIPS may use an API connection to send an IP address to a private entity and receive back location information on where the IP address is being used (e.g. longitude and latitude markers). Similarly, TIPS may send a phone number or address information through an API to receive information on the appropriate state, local, or tribal law enforcement agency or 9-1-1 center to which to route information. Through the APIs, TIPS provides only the minimum information necessary to receive requested information from the external entity. When TIPS receives the information from the external system, the response is automatically added to the TIPS transaction information. The external entity cannot retrieve any additional information from TIPS. NTOS also deployed its own API that allows social media companies to directly submit identified threats to the FBI. The API allows each company to build their own webform which is compatible with TIPS. The API provides the ability to submit details related to the threat along with attachments.

If NTOC personnel determine further investigation is appropriate, the TIEs electronically document the information on a separate complaint form or send the information directly from TIPS to eGuardian, where it will then be migrated to Guardian. If the information falls within the jurisdiction of another federal, state, local, or tribal agency, eGuardian can send the information to the appropriate fusion center for further dissemination. The complaint forms are completed outside of TIPS and sent electronically via Guardian or Sentinel to the appropriate field office for further review and investigatory decisions. There is no direct connection between TIPS and Sentinel. TIPS has a direct connection to eGuardian through which eGuardian reports are generated directly from TIPS. The eGuardian system then migrates the created report directly to Guardian for dissemination to the field.

---

[9] TIPS may contain any information about a subject, victim, or witness provided by a tipster. Typical information provided may include name, address, phone number, email address, and location information. More sensitive information such as a date of birth or social security number may also be provided if pertinent to the tip and known to the tipster.

TIPS may also directly connect with other FBI systems to automate searches. Through machine-to-machine connections, TIPS will send search criteria to the other FBI systems and receive search results of potentially matching information. For searches of classified systems, TIPS will receive an indication (yes/no) of whether the search produced any results. The actual search results are not sent to TIPS.

(g) Connections with Other Systems

The database and web-based application are currently hosted on CJIS UNet . TIPS connects to ETIS. When a call is received, TIPS populates a tip entry in the database by pulling the number from which the call is placed, if available, from the ETIS system. Audio recordings of the calls stored in ETIS can be retrieved by authorized FBI employees from the TIPS entry associated with call recording. In instances where information pertains to an existing case or a recording could further aid in an investigation, the information may be exported from TIPS and shared via email, portable media, or attached to a Guardian Incident. TIPS also receives E-Tips via email. In limited circumstances, TIEs may directly email information from TIPS to other portions of the FBI or to other agencies. TIPS also utilizes API connections with external entities to accept threat information from social media companies and to help TIEs identify location information for potential threats. For example, TIPS uses API connections to receive longitude and latitude markers associated with IP addresses and to attempt to identify the correct local law enforcement agency or 9-1-1 center covering an address or geographic location.

A direct connection between TIPS and eGuardian allows for an eGuardian report to be generated directly through TIPS. The TIEs electronically document information in the TIPS database and directly submit the information from TIPS through the FBI's eGuardian system, to be migrated to the FBI's internal Guardian system on a complaint form. eGuardian also disseminates TIPS data pertaining to state and local matters to appropriate federal, state, local or tribal partners.

TIPS connects directly to LEEP to allow authorized personnel access to the TIPS holdings. Through LEEP, field personnel access actionable and non-actionable written synopses, both electronic and telephonic. LEEP acts as the portal or gateway into TIPS. LEEP can be accessed from a device connected to the internet. As discussed above, TIPS also directly connects to other FBI systems to automate searching of FBI holdings.

(h) Type of System

TIPS is a web-based application within CJIS UNet. CJIS UNet is categorized as an Information System.

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		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify): These numbers are not routinely collected in TIPS unless relevant to a specific complaint. All identifying numbers collected by NTOC are voluntary and callers and E-Tip submitters are not required to provide any information. Anonymous calls and E-Tips are accepted; however, the FBI does capture the IP address of the computer from which an E-Tip is submitted. These IP addresses are emailed to TIPS and retained with E-Tips that are submitted. TIPS also automatically captures the telephone number from which an individual is calling, if available from the phone provider.					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address	X	Medical information	
Gender		Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): All personal data provided to NTOS by callers and e-tip submitters in TIPS is voluntarily provided. Callers and E-Tip submitters are not required to provide any information. Name, address, date of birth, and telephone number are the most commonly collected personal information. Place of birth, gender, alias, age, and race/ethnicity may be collected if they are relevant to a specific complaint. In TTL situations, NTOS may request a subject's identifying information from private companies.					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address	X	Work history	
Work address		Business associates			
Other work-related data (specify): With the exception of a work related email address, these numbers are not routinely collected in TIPS unless relevant to a specific complaint. All information is voluntary and it is unlikely that work-related data would be collected unless it was directly relevant to a complaint**.** For audit purposes, the above information is collected, along					

with the employee's username and associated FBI field office or division.

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

Other distinguishing features/biometrics (specify): All NTOC calls are recorded and stored within the ETIS system, separately from TIPS. The FBI can access the call recordings when necessary for investigative or other authorized purposes; however, the calls are retrieved by text-based searches, not by voice signatures. More information on call recordings is addressed in the ETIS privacy documentation. While voice recordings are not stored in TIPS, they are accessible and exportable through the database.

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

Other system/audit data (specify):

Other information (specify)

NTOC personnel may request limited information from private entities, or obtain information from publicly available sources, in an attempt to identify a potential subject or location of a threat. For example: (1) through API connections, TIPS may push IP addresses, physical addresses, zip codes, or other basic location information to private entities in order to receive longitude and latitude coordinates or information regarding the law enforcement agency or 9-1-1 center covering a specific geographic location; (2) In emergency situations, and under the parameters set forth in federal law, TIEs may provide a username to a social media platform and ask the social media platform to voluntarily provide the user's subscriber information (e.g. name, address, telephone number, email address). Requests for subscriber information are made only in emergency situations and under the parameters set forth in federal law; and (3) TIEs may attach screenshots of relevant information found during open source research and other documentation on the NTOC's handling of a tip.

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	X	Email	X		
Other (specify):					

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

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify):					

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.)

An entry in TIPS begins with information voluntarily provided to the FBI by individuals who are communicating tips, threats, and other issues of concern. Because the information provides public information on individuals and circumstances, it is possible that the information may be inaccurate or incomplete. However, in matters of law enforcement and national security, it is not possible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. Consequently, TIPS retains all information provided. To mitigate the privacy risks associated with collecting inaccurate or incomplete information, the TIEs review all information and make a preliminary determination whether the information should be conveyed for further investigation. No action is taken on the TIPS data alone; rather, the information is provided to the FBI and other agencies only as investigative leads. Information that is not conveyed for further investigation nevertheless remains in TIPS as an administrative record of tip information the FBI has received and because the information in TIPS may be relevant in the future as threats and investigations evolve. To further protect privacy, if, at the time the information is received, the

information is deemed nonactionable, the TIEs must determine whether the information contains solely First Amendment protected activity (e.g. expresses solely freedom of speech, religion, or association, with no indication of a threat). If information is considered to contain solely First Amendment protected activity, no database queries should be conducted and the TIE adds the following caveat to the TIPS transaction: "At the time this tip was provided it was determined to contain solely First Amendment protected activity. No investigative action should be taken with regard to this information alone."

The retention of personally identifiable information (PII) received from tip line callers and E-Tip submitters presents privacy risks of improper access to the data or misuse of information in TIPS. Privacy risks are mitigated through training and controlled access with user identification and two-factor authentication procedures. System users leverage two-factor authentication at the workstation operating system and rely on role-based controls as well as access control lists to interact with the TIPS web-based application. System database access is restricted to administrators who must leverage two-factor authentication and role-based controls to access the database. Direct access is limited to FBI personnel with a need to access the database in performance of their duties. Access is controlled by designated points of contact within NTOS who review access control lists when employees join or leave NTOS. All database activity is recorded and stored in centralized audit logs. TIPS Audit logs are reviewed for possible misuse of the system by the CJIS UNet SSA or ISSO weekly and can be further reviewed upon supervisor request or when a concern about access or use is raised. TIPS also allows authorized FBI personnel to designate sensitive information as restricted. Information marked as restricted is not available to all TIPS users and is only viewable by individuals who have the corresponding TIPS user role which allows a user the ability to designate and view the restricted files. TIPS users who do not have this role designated are able to see that the transaction exists in TIPS, but they are not able to view the information within the transaction. These files include reports of employee misconduct; litigation holds; and, under some circumstances, public corruption.

The retention of additional personal information presents a correspondingly increased risk that the FBI will be maintaining more information that is subject to loss or unauthorized use. The risk of loss/unauthorized use is mitigated by the strong system, user, site, and technical security features present in the database including full database encryption. Collection of data is also limited to only that information necessary and relevant for law enforcement and national security investigations. As explained in Section 1, more detailed information is transferred to the Guardian, eGuardian, or Sentinel systems where the information is analyzed by trained agents and analysts, in accordance with legal and policy requirements for FBI investigations.

Section 3: Purpose and Use of the System

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

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities

X	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
	Other (specify):		

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.

As listed below, the FBI has statutory authority to investigate federal crimes, including crimes of terrorism. Information from the public is essential for the FBI to successfully deter and investigate crime. NTOC supports the FBI's mission by providing consistent and accessible means for the public to provide information that, in turn, permits FBI agents and analysts to follow-up on legitimate leads. On a limited scale, NTOC may attempt to obtain information from submitters or other entities to facilitate processing the information provided by the public and to appropriately act on or refer that information to FBI or other law enforcement entities. . The NTOC staff receives training on the criteria for federal crimes and threats to national security, TTL, suicide intervention skills, interviewing techniques and probative questions, database usage, and report writing. As discussed in Section 1, as appropriate NTOC will forward such complaints to Guardian for further investigation. However, even if a complaint does not result in the submission of a complaint form, the information in TIPS may be relevant in the future as threats and investigations evolve.

TIPS provides important documentation of all complaints that are made to the FBI's central telephone and internet tip lines. In this way, TIPS provides the FBI with a source for internal statistics, such as call volumes from certain locations or the prevalence of certain types of complaints. This information allows the FBI to allocate resources more effectively.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 U.S.C. 533, 534
	Executive Order	
X	Federal Regulation	28 CFR 0.85
	Memorandum of Understanding/agreement (MOU/MOA)	

	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.)

The TIPS data will be retained in accordance with the applicable retention schedules approved by the National Archives and Records Administration (NARA). Information submitted to TIPS and the corresponding audio recordings are saved for 5 years. See NARA Job Number N1-065-05-7, available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-05-007_sf115.pdf. Information and recordings determined to be of investigative value are sent to Sentinel or Guardian and maintained in accordance with the applicable retention schedule approved 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.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

TIPS is subject to extensive security protections, access limitations, and quality control standards. Administrative access to the database is controlled through user identification and two-factor authentication procedures. System user access to the web-based application is authorized following identification and two-factor authentication to the workstation.

Only authorized FBI personnel have access to TIPS. To receive access to TIPS, FBI personnel must contact the designated NTOS points of contact who verify the need for access. Upon notification that an employee has left NTOS and is no longer processing NTOS work, the designated NTOS points of contact terminate the user's access. The access control list for TIPS is reviewed when employees join or leave NTOS. The database stores information in audits logs regarding the search and retrieval of the information. Audit logs are used to recreate the history of a specific TIPS transaction and the actions taken regarding that transaction. Dissemination of information is linked to the authorized user and the identity of the recipient of the information to ensure dissemination was necessary and relevant to the user's official duties. TIPS access logs are reviewed weekly by the SSA or ISSO and can be further reviewed upon suspicion of system misuse.

In addition, annual training regarding the collection, use, protection, and dissemination of information is mandatory for all TIPS users. All TIPS users complete information security and privacy training. The training addresses the roles and responsibilities of users of FBI systems and raises awareness of the sensitivity of the information contained therein and how it should be handled to protect privacy and civil liberties.

PII Confidentiality Risk Level: ☐ **Low** ☑ **Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls. There is no ability to access underlying database without the front-end interface.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit access to PII.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
	Remote Access: remote access is prohibited or limited to encrypted communication channels.
	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching access authorizations to contractual/MOU/MOA restrictions.
	Access Control for Mobile Devices: data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.
Contracts, MOUs and MOAs are not applicable to TIPS. Only FBI personnel can access TIPS. Mobile device access is available for users accessing the read-only version of the TIPS database via LEEP. TIPS is only viewable and accessible in LEEP to individuals who access LEEP with an FBI identity provider (IdP). Regardless of an individual's user role designated in TIPS, if a user accesses TIPS via LEEP they will only have read-only capabilities.	

Audit controls

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

Identification and Authentication controls

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

Media controls

X	Media Access: access to system media (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted and 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
X	Protection of Information at Rest: information stored on a secondary storage device (hard drive or backup tape) is encrypted.

Information System Monitoring

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Private sector	X			
Foreign governments				
Foreign entities				
Other (specify):	X			As discussed in Section 1, limited information may be provided to NCMEC.

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.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

At this time, TIPS cannot be directly accessed by anyone other than FBI personnel. FBI personnel have access to the TIPS database via CJIS UNet or LEEP. LEEP serves as a federated gateway to connect only authorized users to the TIPS database. The TIPS icon on LEEP is only viewable to FBI personnel. This function provides an additional layer of information security. Once LEEP authenticates the field personnel user identity, they will have read-only access to the TIPS holdings, which means that field personnel will be able to search, retrieve, and view TIPS data, but they will not be able to change TIPS data or create or delete TIPS entries. NTOS personnel accessing TIPS via LEEP will have full access to the system. As further explained in Section 1, for those complaints requiring additional investigation, the information is appropriately transferred to other FBI systems for review by the assigned case agents and analysts. On a case by case basis, information from TIPS may be shared within the FBI or with federal, state, local, or tribal partners if the information is pertinent to an investigation in their AOR. When information does not fall into the FBI's jurisdiction, it is shared with federal, state, local, and tribal partners, directly to the AOR believed to have jurisdiction over the matter reported. These agencies do not have direct access to TIPS; rather, information is passed to the agency by an NTOC employee via telephone, email, and/or direct tip submission; an eGuardian report; or an FBI field office.

NTOC personnel may provide limited TIPS information to private entities while attempting to identify a potential subject or location of a threat. Through API connections, TIPS may push IP addresses, physical addresses, zip codes, or other basic location information to private entities in order to receive longitude and latitude coordinates or information regarding the law enforcement agency or 9-1-1 center covering a specific geographic location. Information TIPS pushes through API connections does not contain substantive information about a lead or directly identifying information about a complainant, witness, or subject (e.g. name, date of birth). In emergency situations, NTOC personnel may provide usernames or other identifiers to private entities to determine the identity of an individual making a threat. For example, TIEs may provide a username to a social media platform and ask the social media platform to voluntarily provide the user's subscriber information (e.g. name, address, telephone number, email address). These requests are made only in emergency situations and under the parameters set forth in federal law. For more information about the technical safeguards protecting TIPS see Sections 2.3 and 3.5 above and Section 6.2 below.

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: A pre-recorded message informs the caller that the call may be recorded or monitored. This message states: "During this call, you will be asked to provide identifying information about yourself and/or the persons about whom you are calling. We use this information to assist in your tip. You do not have to provide your name or other personal information; however, that lack of information may delay or hurt our ability to investigate your tip. Any information you provide may be used for authorized purposes." Also, the caller is aware that the TIE is recording relevant information in order to appropriately follow-up on the lead. This PIA also provides notice. The email submission form on the <tips.fbi.gov> website includes a Privacy Act statement and links to the FBI Website Privacy Policy, both of which inform submitters of the purpose of the website and how their submitted information will be used.
X	No, notice is not provided.	Specify why not: Subjects reported in submitted leads do not receive direct notice that their information is being collected and used by the FBI. The information submitted is provided from the public and used for authorized law enforcement and national security purposes. This PIA and the applicable System of Record Notices notify subjects of FBI investigations and tips that the FBI will collect and use their information.

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: All callers and E-Tip submitters voluntarily contact the FBI/NTOC

		and may limit any information provided or terminate the call.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Subjects reported in submitted leads do not have the ability to decline their information being provided to NTOC. The information submitted is provided from the public, or from private entities upon request, and used for authorized law enforcement and national security purposes.

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: All callers have voluntarily contacted NTOC and may limit any information provided or terminate the call. E-Tip submitters are voluntarily sharing information with the FBI. Information provided to the FBI may be investigated pursuant to the FBI's authorities. It is not feasible to have callers and E-Tip submitters or subjects of leads consent to particular uses of the information for law enforcement and national security investigations.

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.

A general notice of the types of records contained in TIPS is provided through publication of a System of Records Notice (SORN). Since the telephone calls and E-Tips provide leads for

investigative purposes, information from these calls and E-Tips are part of the FBI's investigative case management system. The SORN mitigates the risk that individuals may be unaware of how their information could be used if they are involved in or associated with an event related to the collection of law enforcement or national security information. In addition, a pre-recorded message automatically plays when an individual calls NTOC advising the caller of why the phone call is recorded. This message states: "During this call, you will be asked to provide identifying information about yourself and/or the persons about whom you are calling. We use this information to assist in your tip. You do not have to provide your name or other personal information; however, that lack of information may delay or hurt our ability to investigate your tip. Any information you provide may be used for authorized purposes." The TIE may also provide the caller with additional notice that his/her information is voluntary and that it may be further investigated by the FBI. The caller may terminate the call before connecting with the TIE or at any time thereafter. The email submission form on the <tips.fbi.gov> website contains a Privacy Act statement and links to the FBI Website Privacy Policy, both of which inform submitters of how their information will be used.

Subjects reported do not have the ability to decline their information being provided to NTOC. The information submitted is provided from the public and used for authorized law enforcement and national security purposes.

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: TIPS is maintained utilizing Microsoft Windows Server based products which reside on CJIS UNet.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Full testing on CJIS UNet, in which TIPS is housed, was performed on in April 2019. The database is monitored quarterly to ensure safeguards remain in place, with most recent testing in April 2020.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: CJIS UNet ATO dated July 15, 2019, which is the platform housing TIPS. TIPS inherits CJIS UNet's accreditation.
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: Logs pertaining to TIPS activity are correlated within the database server logs. Log content pertains to TIPS user actions via the web-based application interface. Successes as well as failures are captured. Level of logging is commensurate with CNSSI 1015 requirements.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

All workstations and servers that access this information are secured in accordance with the FBI Office of the Chief Information Officer (OCIO) requirements and are verified prior to establishing network connectivity. In addition, all hardware is housed within the FBI facilities that have achieved site security accreditation. Only authorized FBI personnel and/or contractors may have access to the system.

The information/data is further protected by role-based access controls, and Access Control List(s) at the group and individual level. Access Control Lists are reviewed when employees join or leave NTOS. All users are uniquely identified and authenticated. Only FBI personnel may handle the data entered into TIPS, but they are prohibited by virtue of rights assigned to their roles from directly interacting with the system database. Only database system administrators may directly manage the database. Separation of duties precludes database system administrators from working with the information NTOC enters into the database without authorization from a unit chief or section chief.

Logging and auditing procedures are performed as required and appropriate with the FBI OCIO policies. Logs are online for 30 days and archived for a minimum of one year. Audited events are configured at the workstation, server, and database levels. All user activity (successes and failures) is captured. Log information is centralized (read-only) within CJIS Shared Enterprise Network (CJIS SEN) RSA Security Analytics devices. The SSA or ISSO review CJIS UNet logs daily and all system logs, including TIPS, are reviewed weekly. The TIPS-specific audit logs are reviewed weekly by the SSA or ISSO and can be further reviewed upon suspicion of system misuse.

Transmission of information is protected from external threat by the CJIS SEN as documented in RiskVision. All internal network communication and data transmission is controlled and monitored by the CJIS SEN.

The risk of unauthorized access and disclosure is further mitigated because the maintenance and dissemination of information must comply with provisions of any applicable law, regulation, or policy, including the Privacy Act. For instance, the Privacy Act obligates the FBI to make reasonable efforts

to ensure the information that it disseminates is accurate, complete, timely, and relevant, reducing the risk of harm based on any subsequent disclosure of the information.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: *The FBI Central Records System*, **JUSTICE/FBI-002**, 63 Fed. Reg. 8659, 671 (Feb. 20, 1998), as amended at 66 Fed. Ref. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); and *Correspondence Management Systems (CMS) for the Department of Justice*, **JUSTICE/DOJ-003**, 66 Fed. Reg. 29992 (Jun. 4, 2001), as amended by 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), 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.

For purposes of access and retrieval, TIPS makes no distinctions based upon an individual's citizenship or lawful status. Information retrieval is performed by authorized FBI personnel using biographic data (name, DOB, etc.) and keywords, which include the identifying particulars of individuals, to search the database from the web-based user interface.