# Federal Bureau of Investigation

# Privacy Impact Assessment
for
[eGuardian]

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: September 19, 2022

*(May 2019 DOJ PIA Template)*

## Section 1: Executive Summary

The eGuardian System (eGuardian) is a web-based platform where federal and state law enforcement entities can collaborate, coordinate, and deconflict investigative activity. eGuardian allows other federal agencies, state, local, tribal, and territorial law enforcement (FSLTT) entities, the Department of Defense, and Fusion Centers (FCs)[1] (collectively, "Participating Agencies") to document, share and track potential threats, suspicious activity, and cyber, counterterrorism, counterintelligence, or criminal activity (collectively, "Incidents") with the FBI and with each other. The eGuardian user community consists of FBI employees, contractors and detailees, as well as Participating Agency employees, contractors and detailees who have been approved for access by the FBI's Office of Partner Engagement (OPE). eGuardian is hosted in the Amazon Web Services (AWS) unclassified cloud fabric (GovCloud). Users access eGuardian through the FBI's Law Enforcement Enterprise Portal (LEEP), using their LEEP access credentials.[2] The information collected, maintained, used and disseminated by the system describes Incidents and Incident subjects, victims and witnesses. Users can manually input Incidents into eGuardian, or Incidents can be created using systems that interconnect with eGuardian, as described in Section 2. eGuardian information can be retrieved by keyword or index search.

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

## Section 2: Purpose and Use of the Information Technology

As noted above, eGuardian allows Participating Agencies to document, share, and track Incidents with the FBI and with each other. The FBI also uses eGuardian to share information from the FBI's Guardian System (Guardian)[3] and National Threat Operation Center (NTOC) Threat Intake Processing System (TIPS)[4] with Participating Agencies, and to share information from TIPS and InfraGard[5] with

---

[1] FCs are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information among FSLTT. FCs are focal points for information sharing and function as an additional layer of review to confirm that an Incident warrants being entered into the eGuardian system. With the proper training of personnel who perform eGuardian system management and analytical functions, the use of FCs as an intermediary has led to an effective and standardized vetting process that moves Incidents quickly through the eGuardian system.

[2] LEEP is subject to separate privacy documentation. All FBI privacy documentation can be found at: https://www.fbi.gov/services/freedom-of-informationprivacy-act/department-of-justicefbi-privacy-impact-assessments.

[3] Guardian is the FBI's central system for tracking and assigning for investigation criminal and national security threats. Guardian is subject to separate privacy documentation.

[4] TIPS is the primary communications channel for the public to provide information ("tips") to the FBI pertaining to federal crimes, threats to national security, and threats to life (TTLs). TTL tips contain information about a threat to human life (imminent or potential), serious bodily injury, or significant violent action. TIPS is subject to separate privacy documentation.

[5] InfraGard is a partnership between the FBI and members of the private sector to identify emerging technologies and mitigate cyber threats. InfraGard is subject to separate privacy documentation.

Guardian.

Users access eGuardian through the Law Enforcement Enterprise Portal (LEEP), using their LEEP access credentials.[6] LEEP users that have been approved for eGuardian access by OPE can then navigate to the eGuardian home page. From the home page, users can navigate to the following tabs: INCIDENTS, SEARCH, REPORTS, MAPS, ADMIN, FEEDBACK, PRODUCTS and HELP.

**INCIDENTS** allows users to manually create new Incidents and track the workflow of existing Incidents. eGuardian Incidents may be in DRAFT, SHARED, REPORTED, CLOSED, IMPORTED, IN PROCESS, ROUTED or DELETED status.

> DRAFT – When a Participating Agency user initially enters an Incident in eGuardian, the Incident is only visible to the user and the user's supervisor at the Participating Agency.[7] The Participating Agency (user/supervisor) makes the determination whether to SHARE, REPORT or DELETE the Incident. If the Participating Agency deletes the Incident prior to sharing, the FC, the FBI, and other Participating Agencies will not have access to the Incident. If the Participating Agency elects to submit the Incident to their FC Approver, the Incident will display as "DRAFT (FC Approval)," which indicates that it is in DRAFT form, pending approval to be SHARED or REPORTED. If the Participating Agency does not have a relationship with a FC, the draft will be sent to OPE's Approver (eFC Approver, the FBI HQ administrator responsible for FBI HQ user access), and the system will display "DRAFT (eFC Approval)," which indicates that the Incident is pending FBI approval to be SHARED or REPORTED. The DRAFT Incident cannot be viewed or searched by other Participating Agencies or the FBI until the FC Approver or eFC Approver determines that the Incident meets the criteria to be SHARED or REPORTED. The FC or eFC Approver can CLOSE or DELETE the Incident.
>
> SHARED – an Incident that has been determined by the FC or eFC Approver as meeting the criteria for being shared with all Participating Agencies and the FBI. See Appendix A for Criteria. All eGuardian users are able to retrieve, read, and add additional content to (but not edit) SHARED Incidents. When an Incident is SHARED, it is also automatically uploaded to Guardian, where Guardian users (FBI special agents or intelligence analysts) review the Incident to determine whether it warrants further investigative activity by the FBI pursuant to the FBI's Domestic Investigations and Operations Guide (DIOG). Guardian investigative activity concludes with a disposition of "Yes," "No," "Inconclusive," or "Undetermined" nexus to terrorism, cyber, or criminal activity. Unless the Incident has been restricted in Guardian, this disposition is automatically passed to eGuardian, which in turn appends the Incident disposition in eGuardian.[8]

---

[6] LEEP access credentials are granted to FBI personnel as well as federal, state and local law enforcement partners. LEEP is subject to separate privacy documentation.

[7] While FBI users have the ability to input Incidents into eGuardian, the primary purpose of eGuardian is for other law enforcement entities to share information among themselves and to report incidents to the FBI for further vetting, including potential FBI action if warranted.

[8] The Guardian review and adjudication process are not part of this process or document.

REPORTED – an Incident that has been determined by the FC or eFC Approver as warranting FBI review to determine whether it warrants further investigative activity by the FBI, but that also needs to be closely held to preserve investigative equities. All REPORTED counterintelligence Incidents are automatically uploaded to Guardian for FBI review, but are not made available to other Participating Agencies. The FBI then examines the Incident in Guardian to determine whether it warrants further investigative activity by the FBI pursuant to the FBI's DIOG. As with SHARED unrestricted Incidents, the Guardian investigative disposition is automatically passed to eGuardian, which in turn appends the Incident disposition in eGuardian. All other REPORTED incidents are automatically uploaded to Guardian for FBI review and are made available to the appropriate personnel at Participating Agencies.

CLOSED – an Incident which has been reviewed and determined by the Fusion Center Approver to have no nexus to terrorism, cyber, or criminal activity. The Incident is not made available to other Participating Agencies or uploaded to Guardian for FBI review.

DELETED – a Prohibited or duplicated Incident. See Appendix B for Prohibited Incidents. If such an Incident has not been SHARED or REPORTED, it will be deleted by the FC or eFC Approver, otherwise it will be deleted by the FBI. Deleted Incidents are immediately purged from eGuardian. An Incident which has been SHARED or REPORTED will remain in Guardian pursuant to the applicable National Archives and Records Administration (NARA) federal records retention schedule.

IMPORTED – Guardian Incidents that are shared with eGuardian. Sharing of IMPORTED Incidents is permitted on a case-by-case basis, but Incidents related to ongoing FBI investigative activity will generally not be shared. While classified information is not permitted to be entered into eGuardian, as detailed in Appendix B, as an additional precaution, Guardian conducts a text search to alert the sender of possible classified material contained within the Guardian Incident before it is imported to eGuardian.

ROUTED – Threat to Life (TTL) Incidents created by NTOC TIPS to Participating Agencies and REPORTED to Guardian are classified as ROUTED Incidents.

IN PROCESS – Incidents opened in eGuardian that have been SHARED or REPORTED to Guardian and are currently being assessed by Guardian users.

In addition to manual entry, eGuardian Incidents can be created using systems that interconnect with eGuardian. These systems are Participating Agency internal Incident tracking systems, the FBI NTOC's TIPS, and InfraGard.

**SEARCH** allows users to perform a keyword search of Shared Incidents.

**REPORTS** provides access to a menu for where pre-defined reports as described below can be printed.

**MAPS** allows Incidents to be plotted as, or retrieved from, a map location, using incident address, subject address and witness address. (One Incident can be mapped or retrieved at up to three different locations based on the various addresses.)

**ADMIN** provides access to eGuardian's administrative functions such as an individual's eGuardian user profile and allows users to create a customized email subscription service to receive notifications of new Incidents or status-changes of existing Incidents. Email subscribers can only receive information about Incidents to which they would otherwise have access.

**FEEDBACK** allows users to provide eGuardian software enhancement recommendations directly to the eGuardian system development team.

**PRODUCTS** is a library of reports, documents, and other eGuardian reference materials, such as eGuardian user guides, system update information, unclassified law enforcement intelligence and activity reports.

**HELP** provides access to the eGuardian user manual, release notes, and training materials.

The eGuardian user community consists of FBI employees, contractors and detailees, and Participating Agency employees, contractors and detailees who have been approved for access by OPE.

Access to eGuardian is role-based, as set forth in the chart below. eGuardian also provides a read-only role for users that will not be entering Incidents but otherwise meet the requirements for access.

| Role | Incidents | Search | Reports | Admin |
|---|---|---|---|---|
| **General Participating Agency User (Any Participating Agency eGuardian user who can submit and search incidents)** | Add Incidents, Edit own Incidents, Add Attachments, Submit Incident | Search own Incidents, Incidents Reported from user's Agency, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | Compile, Search and View all Reports | Edit My Profile (which allows a user to make changes to their own eGuardian profile), View Contacts, Manage Subscriptions & Notifications |
| **General FBI User (Any FBI eGuardian user who can submit and search incidents)** | Add Incidents, Edit own Incidents, Add Attachments, Submit Incident | Search own Incidents, Incidents Reported any Agency, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | Compile, Search and View all Reports | Edit My Profile (which allows a user to make changes to their own eGuardian profile), View Contacts, Manage Subscriptions & Notifications |
| **Agency Supervisor (Supervisor responsible for reviewing the** | Add Incidents, Edit own Incidents, Add Attachments, Review Incidents, | Search own Incidents, Incidents submitted for approval, Incidents | Compile, Search and View all Reports | Edit My Profile, View Contacts, Manage Subscriptions & |

| | | | | |
|---|---|---|---|---|
| **incidents before they are submitted to the FC to be routed or shared)** | Approve Incidents | Reported from user's Agency, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | | Notifications |
| **FC Approver (FC Supervisor responsible for reviewing incidents submitted by subordinate Participating Agencies to be shared or reported)** | All General User Privileges, Share Incidents, Close Incidents, Report Incidents to Guardian | Search own Incidents, Incidents submitted for approval, Incidents Reported from user's Agency, Incidents reported by Agencies subject to FC coordination, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | Compile, Search and View all Reports | Edit My Profile, View Contacts, Manage Subscriptions & Notifications, Generate Admin Reports, Maintain local FC Contact List (list of Participating Agencies that report to the FC) |
| **FC System Administrator** | All General User Privileges | Search own Incidents, Incidents submitted for approval, Incidents Reported from user's Agency, Incidents Reported by Agencies subject to FC coordination, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | Compile, Search and View all Reports | Edit My Profile and other users' profiles, Create and edit eGuardian Participating Agencies and workflow, Create / Delete Alerts, View Contacts, Manage Subscriptions & Notifications, Generate Admin Reports, Maintain local FC Contact List (list of Participating Agencies that report to the FC). |
| **eFC System Administrator (FBI HQ administrator responsible for user access for FBI HQ users)** | All General User Privileges, Share Incidents, Close Incidents, Report Incidents to Guardian | Search own Incidents, Incidents submitted for approval, Incident's Reported from user's Agency, Incidents Reported by Agencies subject to FBI HQ coordination, and all | Compile, Search and View all Reports | Edit My Profile and other users' profiles, Create and edit eGuardian Participating Agencies and workflow, Create / Delete Alerts, View Contacts, |

| | | | | |
|---|---|---|---|---|
| | | Shared Incidents using Simple (Agency, Location, Status) and Custom Search | | Manage Subscriptions & Notifications, Generate Admin Reports, Maintain local FC Contact List (list of Participating Agencies that report to the FC), View audit logs, Upload Products |
| **Organization Level Group Administrator (Organization administrator responsible for the organization user access)** | All General User Privileges | Search own Incidents, Incidents submitted for approval, Incidents Reported from user's Agency, and all Shared Incidents using Simple (Agency, Location, Status) and Custom Search | Compile, Search and View all Reports | Manage Users within Group and Organizations |

Participating Agency user roles are established by OPE in collaboration with the Participating Agency. OPE, through the eFC System Administrator role, exercises administrative oversight of the system, which includes auditing all accounts for appropriate system access and use.

eGuardian provides the ability to utilize a keyword or index search to retrieve Incident information about any individual, including United States citizens or lawfully admitted permanent resident aliens (USPERS). This keyword search capability also allows "all these words" or "match exact phrase" searches.

Users can manually input Incidents into eGuardian. Incidents can also be created using systems that interconnect with eGuardian, as described below.

- Participating Agency Internal Incident Tracking Systems can connect directly to eGuardian through eGuardian's Web Service software, provided those systems meet the FBI's technical and security requirements as enforced by the FBI's Information Technology Applications and Data Division and Criminal Justice Information Services Division. If the Participating Agency's Incident management system allows its users to mark Incidents Shared or Reported, the Incident will begin the transfer process to Guardian immediately upon transmission to eGuardian. Incident dispositions are not automatically transferred back to Participating Agency Incident Tracking Systems, but these systems can generate queries to retrieve Incident status about only those Incidents created from the Agency's Incident Tracking System.

- NTOC's TIPS is NTOC's system for tracking public-reported threats. When NTOC receives a TTL[9] report, NTOC creates a report in TIPS and provides notice to the relevant Participating Agency via landline telephone call. The TIPS TTL report is simultaneously electronically transmitted through eGuardian to the appropriate personnel at the relevant Participating Agency and FBI field office, using eGuardian's Web Services. TIPS also transmits non-TTL NTOC threat reports to Guardian, through eGuardian, using eGuardian's Web Services. However, these reports are not shared with, viewable or searchable by other eGuardian Participating Agencies. TTL Incident status and status updates can be retrieved by querying eGuardian through TIPS. The status of Non- TTL Incidents cannot be retrieved by TIPS.

- InfraGard uses eGuardian's Web Services to send InfraGard cyber threats as Incidents through eGuardian to Guardian and the appropriate Field Office. These Incidents are captured as REPORTED in eGuardian. Incident status cannot be queried through InfraGard.

eGuardian Information is also transmitted to and from Guardian using the FBI's cross domain services. eGuardian information can also be transmitted through the following reports:

- All Agency Report which provides a count of eGuardian Incidents by disposition.
- Agency Report, which provides a count of the number of Incidents created, still opened, notes added after the Report was shared/reported, Incidents approved/deleted by FC, and number of Incidents by disposition, for a user-defined period of time, by selected Participating Agency.
- Dual Routed Threat to Life Dashboard, which provides a count of the TTL Incidents ROUTED from NTOC to a Participating Agency, for a user-defined period of time.
- FC Report, which provides a count of Incidents created/shared/reported, and notes added, by selected FC, for a user-defined period of time.
- FC and Organizations, which provides a list of FCs and the Participating Agencies that report to the FC.
- FC Suspicious Activity Report Performance Report, which provides a count of Incidents of all FCs for a user-defined period of time.
- User Incident Report, which provides a count of user activity by Participating Agency, for a user-defined period of time.
- Organization Operation Report, which sets forth Participating Agencies/Participating Agency Users by approving FC, to assist in identifying active/inactive Participating Agencies and users.
- Organization Share Report, which provides a count of Incidents by eGuardian Participating Agency, for a user-defined period of time.
- Organization Search Report, which provides a count of Participating Agency searches by Participating Agency, for a user-defined period of time.

[9] NTOC also uses eGuardian as a pass-through to submit non-TTL tips directly to Guardian.

- Organization List Report, which provides a list of eGuardian Participating Agencies and contact information.
- User Request Pending Report, which provides a listing of eGuardian user access requests by Participating Agency, for a user-defined period of time.

eGuardian interconnects with the following FBI systems to facilitate information sharing:

- Law Enforcement Enterprise Portal (LEEP), for Participating Agency user access;
- Guardian, to share eGuardian Incidents with the FBI, and to share FBI Guardian Incidents with eGuardian;
- NTOC's TIPS, to receive TTL and non-TTL reports, and allow TIPS to query TTL Incident status;
- Participating Agency Tracking Systems, to allow Participating Agencies to submit Incidents and query Incident status using eGuardian's Web Service application; and
- InfraGard, to receive cyber-related threat Incidents from the InfraGard community.

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

| Authority | | Citation/Reference |
|---|---|---|
| X | Statute | 28 U.S.C. 33, Sec. 533 |
| X | Executive Order | E.O. 12333, Sec. 1.3(b)(20)(A)<br>E.O. 12333, Sec. 1.4(h)<br>E.O. 12333 Sec. 1.5(g)<br>E.O. 13388<br>E.O. 13356 |
| X | Federal Regulation | 28 C.F.R. 0.85(a)<br>28 C.F.R. 0.85(d)<br>28 C.F.R. 0.85(l) |
| | Agreement, memorandum of understanding, or other documented arrangement | |
| | Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is***

***provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<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 | C, D | |
| **Date of birth or age** | X | C, D | |
| **Place of birth** | X | C, D | |
| **Gender** | X | C, D | |
| **Race, ethnicity or citizenship** | X | C, D | |
| **Religion** | X | C, D | |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | C, D | SSNs are not requested by eGuardian but may be provided in the Incident narrative if relevant for identification purposes. |
| **Tax Identification Number (TIN)** | X | C, D | |
| **Driver's license** | X | C, D | |
| **Alien registration number** | X | C, D | |
| **Passport number** | X | C, D | |
| **Mother's maiden name** | X | C, D | |
| **Vehicle identifiers** | | | |
| **Personal mailing address** | X | C, D | |
| **E-mail addresses (personal, work, etc.) Please describe in Comments** | X | C, D | |
| **Phone numbers (personal, work, etc.) Please describe in Comments** | X | C, D | |
| **Medical records number** | X | C, D | |
| **Medical notes or other medical or health information** | X | C, D | |
| **Financial account information** | X | C, D | |
| **Applicant information** | | | |
| **Education records** | | | |
| **Military status or other information** | X | C, D | |
| **Employment status, history, or similar information** | X | C, D | |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | X | C, D | |
| **Certificates** | | | |
| **Legal documents** | X | C, D | |

| (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 |
|---|---|---|---|
| **Device identifiers, e.g., mobile devices** | X | C, D | |
| **Web uniform resource locator(s)** | | | |
| **Foreign activities** | X | C, D | |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | X | C, D | |
| **Juvenile criminal records information** | | | |
| **Civil law enforcement information, e.g., allegations of civil law violations** | X | C, D | |
| **Whistleblower, e.g., tip, complaint or referral** | X | C, D | |
| **Grand jury information** | | | |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | X | C, D | |
| **Procurement/contracting records** | | | |
| **Proprietary or business information** | | | |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |
| ***Biometric data:*** | | | |
| - **Photographs or photographic identifiers** | X | C, D | |
| - **Video containing biometric data** | | | |
| - **Fingerprints** | X | C, D | |
| - **Palm prints** | X | C, D | |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | | | |
| - **Scars, marks, tattoos** | X | C, D | |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | X | C, D | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | | | |
| - **User ID** | X | A, B, C | |
| - **User passwords/codes** | | | |
| - **IP address** | X | A, B, C | |
| - **Date/time of access** | X | A, B, C | |
| - **Queries run** | X | A, B, C | |
| - **Content of files accessed/reviewed** | X | A, B, C | |
| - **Contents of files** | X | A, B, C | |

| (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 |
|---|---|---|---|
| **Other (please list the type of info and describe as completely as possible):**<br>• Social Media Aliases | X | A, B, C, D | |

### *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 | |
| Phone | | Email | | | |
| Other (specify): | | | | | |

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

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

## Section 4: Information Sharing

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

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | | | X | * |
| DOJ Components | | | X | * |
| Federal entities | | | X | * |
| State, local, tribal gov't entities | | | X | * |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | | | | |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | | | | |
| Other (specify): | | | | |

*****As detailed herein, the purpose of eGuardian is to allow Participating Agencies to document, share, and track Incidents with the FBI and with each other. However, access control limitations and privilege restrictions ensure that information is only accessible to those determined by the Participating Agency as having a need-to-know.

***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.***

eGuardian information will not be released to the public for "Open Data" purposes.

## Section 5: Notice, Consent, Access, and Amendment

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

Notice is provided pursuant to the following SORNs: FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); FBI Data Warehouse System, 77 Fed. Reg. 40630 (July 10, 2012), amended by 82 Fed. Reg. 24151, 157 (May 25, 2017).

In addition, the following SORN is also applicable to this system: Department of Justice Information

Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021).

***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.***

eGuardian contains information potentially relevant to or part of predicated criminal investigations, which are generally conducted confidentially. If individuals who were the subjects of these investigations were routinely given the opportunity to voluntarily participate in the collection, use, or dissemination of information regarding such investigations, it would undermine the integrity of the investigation and seriously impair public trust.

***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 seek access to eGuardian information via the Freedom of Information Act, Privacy Act, or other legal process (e.g., legal discovery), after an investigation is closed. However, for the most part, eGuardian contains data potentially relevant to a predicated investigation and may therefore be exempt from disclosure under these legal authorities.

## 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).***

<table>
<tr>
<td>X</td>
<td>
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):<br>
2/9/2022, expires 2/9/2025.<br>
eGuardian has been classified as High risk under FIPS 199.
<table>
<tr><th colspan="6">Confidentiality</th></tr>
<tr><td></td><td>Low</td><td></td><td>Moderate</td><td>X</td><td>High</td></tr>
<tr><th colspan="6">Integrity</th></tr>
<tr><td></td><td>Low</td><td>X</td><td>Moderate</td><td></td><td>High</td></tr>
<tr><th colspan="6">Availability</th></tr>
<tr><td></td><td>Low</td><td>X</td><td>Moderate</td><td></td><td>High</td></tr>
</table>
</td>
</tr>
</table>

| | |
|---|---|
| | **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>eGuardian is interrelated with the FBI's Guardian system, which is a national security system. As such, the summary or release of POAMs would pose risks to the component. |
| | **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:**<br><br>eGuardian use and activity logs are reviewed by the FBI Information Technology Applications and Data Division, Management Applications Section (CMAS), Monitoring and Compliance (CMAC) Team. eGuardian also provides use and activity logs to the FBI Enterprise Security Operations Center. In addition, security incident response and contingency training is required annually for the CMAC Team. |
| 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:**<br><br>eGuardian is audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. Audit logs are reviewed weekly by the Information System Security Officers (ISSOs). Users are subject to account suspension and referral to the Security Division (SecD) for further investigation. |
| 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:**<br><br>OPE provides system training to eGuardian users upon access and as needed based on user questions or system upgrades. System Administrators receive privileged user training on an annual basis. In addition, eGuardian promulgates and audits for appropriate Incident content and sharing, as described in Appendices A and B. |

***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?***

eGuardian stores and transmits data through AWS Accounts owned and controlled by the FBI with additional security measures in place to mitigate breach and other data risks. The FBI defines, enforces, and manages privileged user access policies across AWS. When storage media in AWS is deprovisioned or released, AWS securely wipes it before it is provisioned or assigned to another AWS customer for use. AWS provides several security capabilities, including the following, to increase privacy and control network access:

- Network firewalls built into GovCloud and web application firewall capabilities create private networks with control access to the FBI's specifications.
- Encryption in transit with Transport Layer Security (TLS) across all services.
- AWS Key Management Services to encrypt data at rest, allowing FBI staff to manage encryption keys. Federal Information Processing Standard l40-2 validated Hardware Security Modules prevent access to plaintext keys, even by Amazon staff.
- Visibility into Application Programming Interface (API) calls identifying who, what, and where calls were made to include log aggregation options.
- Alert notifications when specific CPU, memory or disk space thresholds on the environment are exceeded.
- Individual user accounts can be controlled with permissions across AWS resources.
- AWS maintains multi-factor authentication for privileged accounts.

eGuardian's key privacy controls are as follows:

- Access to eGuardian is password-protected and role-based. User groups are based on a defined need to know and a role requiring access to the data. Not all users have access to all data.
- Access to the server is limited to the System Administrators, who receive privileged user training on an annual basis.
- Only System Administrators can make configuration changes to the system. General users do not have permission to make configuration changes.
- FBI users are required to take the Information Security (INFOSEC) Awareness and privacy training on an annual basis.
- eGuardian is audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, potential intrusion and appropriate Incident content and sharing. Audit logs are reviewed weekly by the ISSOs. Users are subject to account suspension and referral to SecD for further investigation.
- User accounts are disabled immediately when eGuardian personnel are no longer actively employed by the program or are found to be using information inappropriately.
- Vulnerability scans are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.
- All data at rest and in transit is encrypted using FIPS 140-2 compliance encryption.

***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.)***

Incidents are retained in eGuardian for no longer than five years from the date the information was most recently edited. However, Participating Agencies may remove their Incidents from eGuardian at any time. eGuardian Incidents shared with the FBI and Guardian Incidents shared with Participating Agencies via eGuardian are retained in Guardian, pursuant to NARA Job N1-065-09-16. Non-actionable Guardian records are retained for five years. Actionable Guardian records are transferred to NARA for permanent retention ten years after Incident closure. eGuardian audit records are retained until business use ceases, pursuant to NARA General Records Schedule 3.2. Business use ceases for audit purposes at the expiration of the Incident retention period. Information in eGuardian is automatically purged at the expiration of the respective retention period.

## 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:***

Notice is provided pursuant to the following SORNs: FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); FBI Data Warehouse System, 77 Fed. Reg. 40630 (July 10, 2012), amended by 82 Fed. Reg. 24151 (May 25, 2017).

## Section 8: Privacy Risks and Mitigation

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

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

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

The type, quantity, and sources of information eGuardian collects, uses and shares are necessary to document, share and track Incidents. The security and privacy administrative, technical and physical

controls are tailored to the confidentiality, integrity and availability requirements of eGuardian information, consistent with the system's purpose to facilitate the collaboration, coordination and deconfliction of investigative activity among federal and state law enforcement entities.

- The privacy risks associated with the collection and maintenance of eGuardian information are overcollection of information, including information protected by the First Amendment, inaccurate information, unauthorized access, and unauthorized disclosures.
- The privacy risks associated with the access and use (sharing, reporting, etc.) of eGuardian information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of eGuardian are the risks of unauthorized disclosures and loss of data.

These risks are mitigated generally by the controls set forth in Section 6.2. The risks of overcollection of information, including the collection of prohibited incidents and information protected by the First Amendment, are further mitigated by policy that prohibits the entry and sharing of such Incidents. These prohibitions are displayed at each user's login and are described in Appendices A and B. Incidents that are entered into eGuardian in violation of this policy are deleted by the FC or eFC Approver and will not be shared. Repeat submissions of prohibited/protected information by a Participating Agency will trigger an OPE audit.

The risks of inaccurate information, unauthorized disclosures and loss of data are further mitigated by the fact that Incidents are not shared by default but must be determined by the FC or eFC Approver as meeting the criteria for being shared with all Participating Agencies and the FBI. The risk of unauthorized disclosures is further mitigated by the fact that eGuardian information is only authorized to be shared if it meets the criteria indicated in Appendix A of this PIA.

## Appendix A

## Criteria for sharing information with Participating Agencies and the FBI

Information shared with Participating Agencies and the FBI must meet the following criteria:

- It must be potentially related to a past activity associated with terrorism; or
- It must be reasonably indicative of pre-operational planning related to terrorism or other criminal activity and have a potential nexus to terrorism. In this context, pre-operational planning describes activities associated with a known or particular planned operation or with operations generally (e.g. terrorist financing not necessarily tied to specific plots); or
- It must exhibit reasonable suspicion that the subject of the information is involved in criminal activity and the information is relevant to that criminal conduct or activity as set forth in 28 C.F.R. Part 23.

## Appendix B

## Prohibited Incidents

1. The following specific categories of information are prohibited by policy from being entered into eGuardian:

    - classified information;
    - information that divulges sensitive methods and techniques;
    - Foreign Intelligence Surveillance Act (FISA) information;
    - grand jury information;
    - federal taxpayer information;
    - sealed indictments;
    - sealed court proceedings;
    - identifying confidential human source information (information that will reveal the identity of a confidential human source); and
    - Title III subject and intercept information; and other legally protected information.

2. In addition, eGuardian policy and user agreements prohibit the entry of incidents based solely on the ethnicity, race, or religion of an individual; solely on the exercise of rights guaranteed by the First Amendment; or solely based upon the lawful exercise of any other rights secured by the Constitution or the laws of the United States.

These restrictions are prominently displayed on the eGuardian splash page.