United States Department of Justice

Justice Management Division

Privacy Impact Assessment
for the
DOJ Personnel Geospatial Dashboard

Issued by:
Morton J. Posner
Acting General Counsel and Acting Senior Component Official for Privacy, JMD

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

Date approved: [March 23, 2022]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

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

The DOJ Personnel Geospatial Dashboard (GEO Dashboard) is a cloud-based web application that provides a centralized visual display of the location of DOJ personnel to DOJ leadership on a need-to-know basis. This visual display allows Department leadership to quickly ascertain whether any Department personnel may be located at or near the scene of an emergency such as a significant weather event, natural disaster, or mass casualty event (hereinafter referred to as a "significant event"). The GEO Dashboard will streamline and replace the current manual process for reporting this data to those with a need-to-know. The GEO Dashboard is stored within the DOJ Office of the Chief Information Officer's (OCIO) Application Hosting environment which is hosted within the Microsoft FedRamp Azure GovCloud environment.

Using the ESRI Geospatial ArcGIS platform, the GEO Dashboard integrates federal employee personnel data from the National Finance Center (NFC) system with traditional geospatial mapping data to visually display where Department personnel may be located.[1] The DOJ OCIO IamDOJ system already collects the NFC data necessary to perform the mapping functions of GEO Dashboard.[2] The GEO Dashboard will re-use this personnel location data from IamDOJ to correlate with the ESRI geospatial data to visually display where an individual may be[3] located. This will be particularly relevant for DOJ leadership when attempting to determine whether any Department personnel may be impacted by a significant event and may require assistance. The key data elements captured in the visual display will be the DOJ employee's name, personal or work email address, personal or work phone number, component office, GS level, duty station, and home address. For DOJ contractors and other personnel (i.e., detailees, interns, and volunteers), the system will also capture name, email address, phone number, component office and home address, only if this information has been provided by the individual to IamDOJ.

In addition to the data collected from NFC, the GEO Dashboard will pull in Virtual Private Network (VPN) data from the DOJ OCIO Security Operations Center Splunk[4] dataset to identify the individual

---

[1] The National Finance Center (NFC) is a federal government agency division under the United States Department of Agriculture that provides human resources, financial and administrative services for agencies of the United States federal government. The Department of Justice (DOJ) provides personnel data to NFC to support its Human Resources Division and associated activities.

[2] IamDOJ is an official system of record within DOJ's Identity, Credential, and Access Management (ICAM) enterprise services. ICAM meets federal and DOJ security requirements to manage identity attributes, permissions, and their associated system accounts for employees at all levels of the enterprise. IamDOJ is covered by separate privacy documentation.

[3] "May be" is used here because the system is not a real time tracking system. It only indicates static data elements like home and work addresses; it does not track actual movement of individuals.

[4] Splunk is a security information and event management (SIEM) tool that is part of DOJ's Cybersecurity tool suite, and is

computers that have connected to the VPN, by both DOJ employees and contractors, to determine their location. VPN data consists of the IP address that is used when the DOJ personnel access the network.

Location is based on the computer's IP address, which is provided by the individual's internet service provider (ISP). If a mobile hotspot is used, the IP address is assigned by the cellular service provider when connected. If the individual is traveling, and the IP address does not change, the location will not change. However, if the connection is lost and then re-connected, the individual may get a new IP address and indicate a new location. Personnel IP addresses are listed in the dashboard and viewed when a user selects a location for a specific user.

The IP address correlates to a city, state, and country, thus providing additional data about where Department personnel are located. VPN data does not conduct real-time monitoring of the location of the individual accessing the network.

Since the GEO Dashboard will store, process, collect, maintain, use, and disseminate personally identifiable information (PII), JMD prepared this Privacy Impact Assessment (PIA).

Section 2: Purpose and Use of the Information Technology

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

With personnel stretching across the globe, it is imperative that Department leadership have a centralized view of where Department personnel may be located in order to identify individuals that could be affected by significant events and require assistance from the Department.

This application will provide a situational awareness dashboard to inform DOJ leadership about potential impacts to personnel from significant events such as weather events or terrorist attacks. DOJ leadership needs to have visibility into Department personnel who may be living near, assigned to work at, or travelling through areas impacted by significant events in order to understand the scale of the potential impact to DOJ operations.

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	5 U.S. Code § 301 44 U.S. Code § 3101
	Executive Order	

used to collect, aggregate, and analyze system events and logs. Included in the data collected within Splunk is VPN connections and user source IP addresses. Splunk is covered by separate privacy documentation.

X	Federal Regulation	28 C.F.R. § 0.77
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal phone number	X	A	May be pulled from IamDOJ if the user voluntarily provided this info.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A	DOJ assigned Laptop Tag
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A	User VPN Data (User IP address and the corresponding city, state, country of the source IP address)
Biometric data:			
- **Photographs or photographic identifiers**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	System users and admins
- **User passwords/codes**			
- **IP address**	X	A	IP address of DOJ personnel
- **Date/time of access**	X	A	System users and admins
- **Queries run**	X	A	System users and admins
- **Content of files accessed/reviewed**	X	A	System users and admins
- **Contents of files**	X	A	System users and admins
Other (please list the type of info and describe as completely as possible):			

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	Online	X

Government sources:					
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): **Data Sources are described in detail below.**					

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

Data Sources:

Personnel Data (IamDOJ): IamDOJ collects data from a variety of sources, including NFC, JSTARs[5], USAccess[6], and other human resource sources to create a profile for each individual supporting DOJ. IamDOJ does not alter the data from these systems, but uses their information to create a more accurate view of the individual. For example, when an employee is on detail, NFC may not change their component or email address, but these changes might be reflected in USAccess. In addition, most contractors are not listed in NFC, however they are identified in USAccess and JSTARs records. The aggregated view of a person in IamDOJ is used to identify the active personnel supporting DOJ, along with their component, email address, home address, duty station, and other elements, if provided in one of the source systems.

VPN Data (Splunk): When Department personnel log into the DOJ VPN, the system captures their computer's IP address and the DOJ Security Operations Center monitors activity for any lawful government purpose including, but not limited to, monitoring network operations, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations. The IP address are then geolocated to a general area (city, state, country).

The key data elements being collected from the VPN data are: name, email, component, IP address, and the city, state and country as identified by the source IP. The VPN collects the IP address at the time that the user connects to the network and this IP address is then geocoded to a city, state and country. Thus, the most precise location data that can be gathered from such VPN data is city location. This data will only be available when the user is accessing the DOJ network through the VPN. Users

[5] JSTARs (Justice Security Tracking and Adjudication Record System) is a DOJ system used to automate tracking of personnel security investigation activities. JSTARS is covered by separate privacy documentation.
[6] USAccess is a GSA-managed, shared service that provides Personal Identity Verification (PIV) credentialing services and support for federal employees and contractors at established locations throughout the country. USAccess is covered by separate privacy documentation.

that are at a DOJ office and directly connected to the network through ethernet are not included in the dashboard.

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	Authorized ODAG and JMD users with a need-to-know can view data and/or the dashboard within the application.
DOJ Components			X	Identified users with a need-to-know within other DOJ components will be provided direct access to the system.
Federal entities	X			Records Officers will share, or transfer, archived records to NARA. DOJ may share documents when responding to requests from Congress or the White House.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

No information from this system will 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.

Prior to obtaining access to Department information systems, users are required to review and sign the DOJ Cybersecurity and Privacy Rules of Behavior for General Users. The Rules of Behavior provide direct notice to the users that they have no expectation of privacy in, and consent to the monitoring of, their use of DOJ information systems. Additionally, users receive indirect notice of the Department's collection of this information through the following System of Records Notices:

- JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021).
    - Individuals are notified that account and audit logs are maintained for the purpose of monitoring system activity.
- JUSTICE/DOJ-009, Emergency Contact Systems for the Department of Justice, last published in full at 69 Fed. Reg. 1762 (Jan. 12, 2004) and amended at 82 Fed. Reg. 24147 (May 25, 2017).
    - Individuals are notified that contact information, including home addresses and where they may be reached while on travel, is maintained for emergency purposes.

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.

Users do not have the opportunity to voluntarily participate in the program. Prior to obtaining access to Department information systems, users are required to review and sign the DOJ Cybersecurity and Privacy Rules of Behavior for General Users which states that users consent to the monitoring of their use of DOJ information systems.

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.

- DOJ employees have access to their NFC data through their Employee Personal Page which allows them to ensure that their information is current and gives them the opportunity to identify any inaccuracies for correction with management.
- Similarly, DOJ contractors can choose to provide their home address or not for inclusion in IamDOJ, and through the IamDOJ Portal they can identify any inaccuracies for correction with the appropriate DOJ points of contract.
- DOJ personnel can access IamDOJ by navigating to the self-service portal to self-report personal contact info, work location, and home address.
- DOJ personnel does not have access to VPN data. The IP address identified upon the user accessing the Department's VPN is obtained automatically through system logs, without manual intervention. The possibility of inaccuracy is very low.

Section 6: Maintenance of Privacy and Security Controls

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

x	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** Expected ATO completion date is March 25, 2022. **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:**
	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:** The system is undergoing a risk assessment and audit logging will be implemented to capture necessary user activity logs as required under DOJ Order 0904, which governs the Department's cybersecurity program.
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:** Audit records will be reviewed and analyzed at least weekly for indications of

	inappropriate or unusual activity, and a record of the audit log will be provided to the system owner and security officer(s).
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:** Basic training will be provided to all users along with a quick reference guide with instructions on how to properly use the system.

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

- The GEO Dashboard application will only allow approved users to access the dashboard via multi-factor authentication (MFA) using their PIV card and on a DOJ-issued computer while connected to the DOJ network. The application will undergo an Authority to Operate (ATO) review and trained information systems security officer (ISSO) staff will perform continuous monitoring,[7] quarterly control reviews, and required system access reviews to reduce the risk of unauthorized access and disclosure and identify any possible unauthorized system access.
- The system has been categorized as FIPS 199: Moderate.
- Users will be trained to operate the system and must complete annual cybersecurity awareness training as required by Department policy.
- Data at-rest and in-transit encryption methods are provided by the Microsoft Azure hosting environment.
- The ISSO and/or Cybersecurity Staff (CSS) policy analysts will perform periodic auditing of privileged user accounts to ensure that users are assigned the correct user role with the fewest privileges necessary to perform their assigned job duties. Only account administrators will be given administrative rights within the system.

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.)

[7] Pursuant to National Institute of Standards and Technology (NIST), information security continuous monitoring is "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." NIST, Special Publication 800-137, September 2011, available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.

The information will be retained for 25 years and disposed of at the end of the retention period by electronic transmission to the National Archives and Records Administration (NARA). Once receipt is confirmed by NARA, the records are removed from the system. These records have been assigned record schedule number DAA-0060-2017- 0002.

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:

JUSTICE/DOJ-002, Department Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec.30, 1999) and amended at 86 Fed. Reg. 37188 (July 14, 2021).

JUSTICE/DOJ-009, Emergency Contact Systems for the Department of Justice, last published in full at 69 Fed. Reg. 1762 (Jan. 12, 2004) and amended at 82 Fed. Reg. 24147 (May 25, 2017).

Section 8: Privacy Risks and Mitigation

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

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

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

When a significant event occurs, it is imperative that Department leadership be able to quickly and accurately determine if any Department personnel may be impacted by the event. While the Department has been manually tabulating this information, it is a time-consuming process. In the event of an emergency, time is of the essence and the GEO Dashboard can quickly and effectively

display the general location of Department personnel across the globe. Importantly, GEO Dashboard will only be used by those who have a specific need-to-know concerning the location of Department personnel. Further, the GEO Dashboard will not collect any additional PII beyond that which is already collected by DOJ. The dashboard will simply re-use this data in a way that serves to visually depict the location of personnel for the purposes of ensuring the overall safety of DOJ personnel and resources.

Privacy Risk: Unauthorized access to the system and/or unauthorized use of the data.
Mitigation: Access to the dashboard and use of the locational information is strictly limited to DOJ users with a need-to-know. Only those individuals will be granted access to the dashboard and given the user role with the least privileges to complete their job duties. The dashboard will only be accessible when connected to the DOJ network which requires multi-factor authentication. Therefore, by design, only DOJ personnel with appropriate clearance will be able to access the system. In addition, the system generates audit logs which will be regularly reviewed for any potential unauthorized access attempts. Further, the project team plans to onboard the system logs to the Justice Security Operations Center's Splunk data so that the information systems security officer and Justice Security Operations Center has access to audit/review administrator/sysadmin actions. This system will be continuously monitored through security control and risk assessments.

Privacy Risk: Data exfiltration of DOJ personnel locational data.
Mitigation: As stated above, users of this system are only granted access if they have a need-to-know to fulfill their job duties and have been granted appropriate privileges within their user role. All users are vetted by DOJ for suitability prior to completing work for the agency. The system also uses FIPS 140-2[8] compliant encryption algorithms to protect that data at-rest and in-transit.

Privacy Risk: Inaccurate aggregation of data.
Mitigation: Users will be provided with training on how to properly use the system to complete their job duties. The GEO Dashboard is reliant on the data sources (NFC data via IamDOJ and VPN automatically collected data) to accurately store the data that is being pulled into each system. Extensive testing has been conducted to ensure that the data is being accurately extracted and displayed on the dashboard.

[8] FIPS 140-2 is a NIST publication that lists security requirements for cryptographic modules protecting sensitive but unclassified information in computer and telecommunications systems.