United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for the
USA Employee Notification System (USAENS)

Issued by:
Senior Component Official for Privacy - Kevin S. Krebs

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: August 22, 2024

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The USA Employee Notification System (ENS) is a comprehensive enterprise-wide notification system used to notify the United States Attorneys' offices and EOUSA employees of emergency and non-emergency situations. The system provides notifications, management announcements and guidance. The system communicates information using phone, electronic mail, and Short Message Service (SMS) text, within the EOUSA and United States Attorneys' community, which includes federal employees and contractors, as well as members of the public whose jobs require them to be physically at a USAO office and has the ability to confirm delivery of notifications.

Additionally, the system provides EOUSA and USAOs the capability to quickly notify personnel in a facility about any emergency that threatens the safety and security of that facility as a part of the communications infrastructure of the facility Occupant Emergency Plan (OEP). In addition, the alerting feature triggers the building marquees to provide a message to facility occupants of an emergency and advise them of protective actions to execute during the emergency.

A PIA is required by Section 208 of the E-Government Act because ENS is a new information technology, which involves the collection, maintenance, and dissemination of information in identifiable form obtained from members of the public, in addition to federal government employees and contractors.

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, or to conduct analyses to identify previously unknown areas of concern or patterns.

USAENS sends notifications and relays messages to internal DOJ federal employees and contractors. Certain non-DOJ individuals such as custodial staff at DOJ facilities are authorized to use the application to sign up for mass notification alerts. These messages are either critical in nature, routine, or for testing purposes with appropriate authorization. In accordance with Executive Order 12656, National Security Presidential Directive (NSPD) - 511, all EOUSA components should have a viable Continuity of Operations Planning (COOP) capability and plan in place that ensures the performance of their essential functions during any emergency or situation that could disrupt normal operations. An effective USAENS solution is a critical part of this plan. The National Response Framework (NRF) requires proactive notification and deployment of federal resources in anticipation of or response to all hazards, threats, and emergencies in coordination and collaboration with state, tribal, and local governments, and with private-sector entities when possible. USAENS uses communications devices (such as phone, text messages, email messages, and desktop Alert) to share important information in accordance with the NRF and other directives. This information is shared with emergency response personnel from EOUSA in the aftermath of a scheduled exercise or disaster and prompts immediate action to resolve or mitigate the all-hazard situation.

DOJ employees and contractors' contact information is pulled from the Enterprise Application Development (EAD) office supported application Case Management Enterprise System (CMES)/Consolidated District Information System(CDIS) which is the user contact information system and may include work email address, work cell phone, personal email address, personal home telephone number, personal cell phone number, approximate mailing address and geolocation (longitude and latitude) of the incident and well as photo of the user triggering the incident if it is provided. Non-DOJ users can use the ENS-Alertus application to input their contact information to receive notifications.

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.C. § 301 • 28 U.S.C. § 547 • 28 U.S.C. Ch. 35 • 44 U.S.C. Chs. 2129, 31, and 33 • Title 41 Federal Management Regulations (FMR) Part 102-193, "Creation, Maintenance, and Use of Records" • Federal Information Security Modernization Act of 2014, 44 USC § 101 note
X	Executive Order	• Executive Order 12656, National Security Presidential Directive (NSPD) - 511
X	Federal Regulation	• Federal Property Management Regulations [41 CFR 101–20.103–4 and 41 CFR 102- 74.230-260] • Occupational Health and Safety Administration (OSHA) Emergency Action Plans and Fire Protection Regulation [29 CFR 1910.38 and 165] • Department of Homeland Security Presidential Directive (HSPD-5(18))
X	Agreement, memorandum of understanding, or other documented arrangement	• Federal Protective Service: Secure Facilities Safe Occupants, Occupant Emergency Plan Guide
X	Other (summarize and provide copy of relevant portion)	• DOJ ORDER 0904, Cybersecurity Program (September 15, 2016)

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*	*C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B and C	First and last name of DOJ employees and contractors pulled from the Case Management Enterprise System (CMES)/CDIS, , other authorized federal government personnel, and authorized non-government users, such as building custodial staff, provide their names when registering for an account.
Date of birth or age	X	A, B	ENS-Alertus app allows federal users the option to input date of birth or age information.
Place of birth	NA		
Sex	NA		
Race, ethnicity or citizenship	NA		
Religion	NA		
Social Security Number (full, last 4 digits or otherwise truncated)	NA		
Tax Identification Number (TIN)	NA		
Driver's license	NA		
Alien registration number	NA		
Passport number	NA		
Mother's maiden name	NA		
Vehicle identifiers	NA		
Personal mailing address	X	A, B and C	ENS-Alertus app, user may input personal mailing address.
Personal e-mail address	X	A, B and C (For C, users are limited to individuals whose job requires them to be physically at a USAO office, and who are invited and approved by USAO.)	ENS-Alertus app, user may input personal email address.

(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, B and C (For C, users are limited to individuals whose job requires them to be physically at a USAO office, and who are invited and approved by USAO.)	ENS-Alertus app, user may input personal phone number.
Medical records number	NA		
Medical notes or other medical or health information	NA		
Financial account information	NA		
Applicant information	NA		
Education records	NA		
Military status or other information	NA		
Employment status, history, or similar information	NA		
Employment performance ratings or other performance information, e.g., performance improvement plan	NA		
Certificates	NA		
Legal documents	NA		
Device identifiers, e.g., mobile devices	X	A, B and C (For C, users are limited to individuals whose job requires them to be physically at a USAO office, and who are invited and approved by USAO.)	Device identifiers are required to process and apply various exemption policies. Only the mobile devices operating system is collected, i.e., iOS or Android, for both business and personal devices.
Web uniform resource locator(s)	NA		
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	NA		
Juvenile criminal records information	NA		
Civil law enforcement information, e.g., allegations of civil law violations	NA		
Whistleblower, e.g., tip, complaint or referral	NA		
Grand jury information	NA		
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	NA		
Procurement/contracting records	NA		
Proprietary or business information	NA		

(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
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C (For C, users are limited to individuals whose job requires them to be physically at a USAO office, and who are invited and approved by USAO.)	Location information will pull from DOJ employees and contractors and members of the public that have the ENS/Alertus app on their phones. Geolocation (longitude and latitude) of the user triggering the incident is pulled from the ENS/Alertus app on their phone.
Biometric data:	NA		
- **Photographs or photographic identifiers**	X	A, B and C (For C, users are limited to individuals whose job requires them to be physically at a USAO office, and who are invited and approved by USAO.)	ENS-Alertus component allows the user the option to upload a photo to their profile. The photo will be encapsulated if the user is the one triggering the panic button. User may also upload photos of the incident scene.
- **Video containing biometric data**	NA		
- **Fingerprints**	NA		
- **Palm prints**	NA		
- **Iris image**	NA		
- **Dental profile**	NA		
- **Voice recording/signatures**	NA		
- **Scars, marks, tattoos**	NA		
- **Vascular scan, e.g., palm or finger vein biometric data**	NA		
- **DNA profiles**	NA		
- **Other (specify)**	NA		
System admin/audit data:	X	A, B	SQL Server and Windows logs capture access info.
- **User ID**	X	A, B	SQL Server and Windows logs capture access info.
- **User passwords/codes**	X	A, B	SQL Server and Windows logs capture access 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
- **IP address**	X	A, B	SQL Server and Windows logs capture access info.
- **Date/time of access**	NA		
- **Queries run**	NA		
- **Content of files accessed/reviewed**	NA		
- **Contents of files**	NA		
Other (please list the type of info and describe as completely as possible):	NA		

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	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	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): State, local, tribal governments cannot initiate their own participation in USAENS. These entities must be specifically invited by USAO and maintained at USAO. If members from the state, local, tribal government do participate, they become sources of the information.					

Non-government sources:					
Members of the public	X	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		X	USAENS utilizes user data that is either imported or manually entered in ENS to support deployment operations and to contact EOUSA users in the event of an emergency. EOUSA components assess the situation and location of a specific incident to determine which responders to activate in a specific scenario. In a scenario when ENS is activated, users receive the appropriate notifications for the scenario via voice calls to phones, text messages, or as email notifications. Users may respond by acknowledging they have received the message and the explanation of what to do as a result. USAENS imports the data from CDIS daily. The service pulls the employee/contractor first and last name, work email address, work cell phone, personal email address, personal home telephone number, and personal cell phone number.
DOJ Components	X			Only if EOUSA invited and approved DOJ Components participate in ENS-USAAlertus Alertus app.

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.**
Federal entities	X			Only for those whose jobs require them to be physically at a USAO office, and who are invited and approved by USAO.
State, local, tribal gov't entities	X			Only for those whose jobs require them to be physically at a USAO office, and who are invited and approved by USAO.
Public	X			Only for those whose jobs require them to be physically at a USAO office, and who are invited and approved by USAO.
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.

This section is not applicable.

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.

JUSTICE/USA-001, Administrative File, last published in full at 48 Fed. Reg. 56662 (Dec. 22, 1983), available at https://www.justice.gov/opcl/docs/48fr56662.pdf.

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records (formerly Department of Justice Computer Systems Activity and Access Records), last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

JUSTICE/DOJ-009, Emergency Contact Systems for the Department of Justice, last published in full at 69 FR 1762 (Jan. 12, 2004), available at https://www.gpo.gov/fdsys/pkg/FR-2004-01-12/pdf/04-583.pdf.

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.

USAENS users may voluntarily download the Alertus mobile application where the user can create their own profile. By doing so, they consent to the collection and dissemination of their information as needed to respond to applicable incidents. Their individual profile will be linked to all incidents reported by that user.

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.

This PIA, along with the SORN, provides notice regarding information correction procedures for USAENS.

JUSTICE/USA-001, Administrative File, last published in full at 48 Fed. Reg. 56662 (Dec. 22, 1983), available at https://www.justice.gov/opcl/docs/48fr56662.pdf.

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records (formerly Department of Justice Computer Systems Activity and Access Records), last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

JUSTICE/DOJ-009, Emergency Contact Systems for the Department of Justice, last published in full at 69 FR 1762 (Jan. 12, 2004), available at https://www.gpo.gov/fdsys/pkg/FR-2004-01-12/pdf/04-583.pdf.

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):** USAENS last authorized on April 30, 2024 and expires on April 30, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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:** N/A
	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:** NIST Moderate baseline controls are implemented.
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:** USAENS generates audit logs for all activities within USAENS. The USAENS Information System Security Officer (ISSO) will be responsible for reviewing all audit logs on a weekly basis.
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:** General information security and privacy training and training specific to the system for authorized users within the Department.

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

Access controls will be implemented to ensure only authorized users have access to the information collected. Also, access will only be granted to those who require the information to accomplish their job duties. USAENS is an internal system under the USAVON GSS network behind the firewalls and DOJ TIC, and interfaces with the USAVON/Active Directory ("AD"). USAENS System are managed by ENS Management Console and USAAlertus system are

manage by USAAlertus management Console that is all connected to AD. All login actions will be audited to ensure that no unauthorized users have been granted access to the system, and all audit logs are reviewed on a weekly basis by the ISSO. An open session within the information system will also be subject to session termination in cases of inactivity to ensure that unauthorized access to the system is not granted and minimize the risk of unauthorized disclosure.

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.)

The data in the USAENS system is maintained for as long as it is needed by the authorized DOJ users and are subject to the respective retention periods that govern them, e.g., NARA General Records Schedules, agency SF-115s, and any applicable SORNs published under the Privacy Act of 1974, 5 U.S.C. §552a (see https://www.justice.gov/opcl/doj-systems-records). Procedures have been developed to ensure that electronic copies are not retained beyond the retention period established for the original records and will be disposed in accordance with DOJ Network Account Records Management USAP No. 3-13.300.004.

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/USA-001, Administrative File, last published in full at 48 Fed. Reg. 56662 (Dec. 22, 1983), available at https://www.justice.gov/opcl/docs/48fr56662.pdf.

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records (formerly Department of Justice Computer Systems Activity and Access Records), last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

JUSTICE/DOJ-009, Emergency Contact Systems for the Department of Justice, last published in full at 69 FR 1762 (Jan. 12, 2004), available at https://www.gpo.gov/fdsys/pkg/FR-2004-01-12/pdf/04-583.pdf.

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?

USAENS is available for use by USAO government and contractor personnel working on behalf of the government or for those members of the public whose job requires them to be physically at a USAO office, and who are invited and approved by USAO. USAENS is an internal system under the USAVON GSS network behind the firewalls and DOJ TIC. USAENS servers and hardware are in both NOC and CEF-DC that is manage under EOUSA GSS USAVON and USAENS engineer/admin. All servers interface with the USAVON/Active Directory and follow the USAVON AD user account management process. USAENS systems are managed by ENS Management Console and USAAlertus. Part of the USAENS system is manage by USAAlertus management Console that is all connected to AD. EOUSA explicitly authorizes access to USAENS security functions to administrators with privileged access.

USAENS users, whether they send or receive activations are always part of AD. USAENS component USAAlertus is distributed more widely, but only EOUSA AD users can send systemwide activations.

The Alertus app also allows users, who are members of the public whose jobs require them to be physically at a USAO office, and who are invited and approved by USAO to signed up to only received notifications. ENS district's System Manager (SM) will provide the code for such users to manually sign up.

EOUSA/Enterprise end user technology (EEUT) and USAENS Program Manager employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with EOUSA missions and business functions. The USAENS Program Manager reviews and approves all authorizations before provided to users. EOUSA utilizes access controls for separation of duties and least privilege. Users are provided only access to systems and/or data required to carry out their duties. Security groups on AD dictate user roles and accesses via security groups. For users who are not in the AD (i.e. members of the public whose job requires them to be physically at a USAO office, and who are invited and approved by USAO), their ENS account will be created manually by a federal user with a code that is giving by the district's DOSM or the District SM.

USAENS utilizes user data that is either imported or manually entered into USAENS to support deployment operations and to contact USAENS users in the event of an emergency. EOUSA components assess the situation and location of a specific incident to determine which responders to activate in a specific scenario. In a scenario when USAENS is activated, users receive the appropriate notifications for the scenario via voice calls to phones, text messages, or as email notifications. Users may respond by acknowledging they have received the message and the explanation of what to do as a result.

The disclosure or sharing of emergency information increases risks to privacy. However, there are measures taken to reduce the risk of unauthorized disclosure and potential data breach. All EOUSA component systems are subject to consistent assessment and authorization processes ensuring that security controls are in place to protect the confidentiality, integrity, and availability of all information

and systems that house the information.

The principle of least privilege will be enforced to ensure those who have access are only granted the minimum access required based on job duties. All EOUSA staff require mandatory security awareness and role-based training on an annual basis. Part of the Alertus app limits non-federal users to only receiving notifications. Such users will not be allowed to initiate an incident.

Additionally, security controls will be tested during the assessment process and prior to system authorization. Other security control families that are tested and implemented as safeguards include: Auditing, Contingency Planning, Incident Response, Media Protection, Physical Protection, Risk Assessment, and System and Information Integrity.