INTERPOL Washington,
U.S. National Central Bureau (USNCB)

Privacy Impact Assessment
for the
ECE Case Management System

Issued by:
Kevin R. Smith, General Counsel,
Senior Component Official for Privacy

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [February 7, 2020]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Interpol Washington, the United States National Central Bureau (USNCB), is authorized by statute and operates within the guidelines prescribed by the Department of Justice, and also pursuant to a memorandum of understanding with the Department of Homeland Security concerning its management by the two Departments.

The mission of the USNCB is to facilitate international law enforcement cooperation as the United States representative to the International Criminal Police Organization (INTERPOL), on behalf of the Attorney General of the United States. Pursuant to 22 C.F.R. 0.34, the major functions of the USNCB are to:

- Facilitate international law enforcement cooperation as the United States representative to INTERPOL on behalf of the Attorney General, pursuant to 22 U.S.C. § 263A;
- Represent U.S. law enforcement at INTERPOL conferences and symposia;
- Support the U.S. representative of the INTERPOL Executive Committee, if any;
- Serve as a member of the Executive Committee of INTERPOL;
- Transmit information of a criminal justice, humanitarian, or other law enforcement-related nature between National Central Bureaus of INTERPOL member countries, and law enforcement agencies within the United States and abroad; and respond to requests by law enforcement agencies and other legitimate requests by appropriate organizations, institutions, and individuals, when in agreement with the INTERPOL constitution;
- Coordinate and integrate information for investigations of an international nature and identify those involving patterns and trends of criminal activities;
- Conduct analyses of patterns of international criminal activities, when specific patterns are observed;
- Process name checks and background records for licensing, security clearance, employment, humanitarian and other law enforcement purposes.

In compliance with federal guidelines, the USNCB has conducted a Privacy Impact Assessment (PIA) of its processing and use of privacy data because this information system, the ECE Case Management System, has undergone significant changes affecting the information in identifiable form collected and maintained by this system. This PIA demonstrates that the USNCB has considered privacy from the initial deployment of the ECE environment and throughout its life cycle. Additionally, this PIA demonstrates that the system owners and developers have made technology choices that reflect the incorporation of privacy into the fundamental system architecture.

Description of the Information System

The USNCB is supported by information systems known as OA/ENVOY and an integrated infrastructure supporting processing and management of USNCB data both on premise and in a government cloud. The USNCB has referred to its legacy case management system as "OA/ENVOY/ECE" (or "ECE") which is considered a distinct application that resides on the OA/ENVOY platform. In this PIA document, "ECE" designates this case management system and its subsequent upgrades.[1]

[1] This PIA only applies to the USNCB's ECE case management system, and does not apply to the INTERPOL system or activities outside the ECE system boundary.

ECE records and manages all international and domestic law enforcement and humanitarian case data and information. Its primary business function is to provide a robust integrated network environment to support USNCB personnel in managing and processing domestic and international law enforcement and humanitarian assistance case information[2], and providing information sharing capabilities to the domestic and international police community. These cases consist of law enforcement documents, images, official forms and records, and business processes surrounding the creation, routing, and manipulation of case and case related data.

ECE collects general personal data about subjects of international criminal investigations such as: Name, Date of Birth, Place of Birth, Gender, Physical Characteristics, Race/Ethnicity, Mother's Maiden Name, etc. Additionally, ECE collects identifying numbers (such as Passport Number and Driver's License Number) as well as Distinguishing (physical) Features and Biometric data. The information is used to support the law enforcement and humanitarian functions performed by the USNCB. ECE manages data on foreign and domestic criminal and noncriminal, humanitarian, and related law enforcement matters. These records are maintained to assist criminal investigations, and support international law enforcement cooperation.

The ECE processing environment consists of an integrated network that includes: hardware, system software, system utilities, and communication interfaces. The two core components of the ECE application consists of a case management system and case document repository.

The ECE case management component allows authorized authenticated users to view and manipulate case data, conduct logical analyses on multiple datasets, upload files, and search on cases and documents. The case management component is a web-based application that supplies a front-end interface to the back-end case document repository component and provides users the tools and functionality necessary to manage and manipulate case data. The application incorporates the pre-defined physical processes that make up the USNCB Case Management Workflow, as documented within the USNCB Caseworkers Manual. Typically, information and cases processed by the USNCB and managed in ECE must be consistent with the provisions of the INTERPOL Constitution, rules and regulations, U.S. law, and the Privacy Act. USNCB staff are responsible for coordinating investigative requests from INTERPOL member countries to the United States, and requests from state, local or federal agencies, for information or action. A request or correspondence related to a request is reviewed and processed by a USNCB caseworker pursuant to established USNCB procedures and guidance.

The ECE case document repository component is designed to manage large bodies of information and is built by leveraging a combination of a file storage repository and a database system for file metadata. The case document repository provides an environment that is both convenient and efficient for USNCB analysts to store and retrieve information.

Furthermore, the ECE case management system and case document repository both leverage government cloud services for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) in

---

[2] The managing and processing of humanitarian case data includes assistance in non-criminal investigative matters such as health and welfare checks on suicide threats, missing persons, assistance in cases involving natural disasters and in other related matters.

order to provide an Enterprise Solution for USNCB, ensuring a robust infrastructure, content security, availability and disaster recovery.

The ECE user community consists of USNCB investigative analysts, agents, contractors, and interns. The investigative analysts are permanent employees within the Department of Justice. The agents are detailed from participating U.S. state, local, federal and tribal law enforcement organizations as representatives of their respective organizations and provide investigative support to the USNCB. Only those individuals specifically authorized have access to the USNCB records. USNCB only grants access to records to those individuals who require access to perform official duties. There are no outside users permitted access to ECE, including personnel from the larger DOJ community.

Information may be entered into the system in several ways. Information can be manually entered by USNCB analysts, and documents can be scanned or uploaded into the system. Information is retrieved primarily by name, case number, personal identification numbers, passport numbers, and by weapon serial number or motor vehicle identification number. All information is accessed via web browser and database authentication mechanisms.

All information is communicated via secure channels. Lastly, information can be electronically transmitted to the system via email. Information is transmitted from the system via investigative correspondence which become emails. ECE communicates with federal, state, local, and tribal law enforcement organizations through secure VPNs and Nlets and with INTERPOL member countries through the INTERPOL I/24-7 police communications system administered by the INTERPOL General Secretariat in Lyon, France. Access to the emails generated by ECE is limited to authorized officials in the U.S. and in INTERPOL member countries who are recipients of the emails and who do not otherwise have access to ECE or the USNCB records contained in ECE. The emails will only be sent to contacts who have been vetted in advance of requests. The list of approved contacts is actively curated to ensure accuracy and timeliness. In addition, ECE generated emails provide law enforcement data to other federal law enforcement agencies for inclusion in their systems (e.g., Fingerprint files are transmitted to FBI-CJIS and DHS.)

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.

The major functions of the USNCB are to:

- Facilitate international law enforcement cooperation as the United States representative to INTERPOL;
- Transmit information of a criminal justice, humanitarian, or other law enforcement-related nature between National Central Bureaus of INTERPOL member countries, and law enforcement agencies within the United States and abroad; and respond to requests for criminal investigative assistance by law enforcement agencies and other legitimate requests by

appropriate organizations, institutions, and individuals, when in agreement with the INTERPOL constitution;
- Coordinate and integrate information for investigations of an international nature and identify those involving patterns and trends of criminal activities;
- Conduct analyses of patterns of international criminal activities, when specific patterns are observed.

In support of these mission goals, the USNCB collects, coordinates, compares, analyzes, researches, and integrates criminal information for investigation and eventual prosecution of suspected individuals involved in criminal cases of an international nature. All information collected, processed, and/or used is to facilitate the sharing of information between federal, state, local, and tribal law enforcement-related authorities in the United States, and foreign authorities engaged in law enforcement functions including: the investigation of crimes and criminal activities, obtaining evidence, the sharing of law enforcement techniques, prevention of crime assistance in humanitarian matters, the location and arrest of fugitives and wanted persons, the location of missing persons, border and immigration control, assistance in litigation, the sharing of criminal history and background information used for investigative purposes, determinations regarding the suitability of applicants for law enforcement and non-law enforcement-related employment, and the issuance of a license, grant, contract, or benefit.

Additionally, the USNCB is also responsible for generating metrics and statistics regarding trends of international crime activities. It then reports those trends to appropriate local, state, federal, and INTERPOL member country law enforcement authorities. In support of this mission responsibility, the USNCB may incorporate minimal privacy information.

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	22 U.S.C. Section 263a
	Executive Order	
X	Federal Regulation	28 C.F.R. 0.34
X	Agreement, memorandum of understanding, or other documented arrangement	MOU with Department of State pertaining to stolen and lost passport numbers; and Interconnection Security Agreement Addendum (ISAA-2015-12-296) with U.S. Customs and Border Protection Constitution of the International Criminal Police Organization-INTERPOL[3] General Regulations of the International Criminal Police Organization-INTERPOL[4]

[3] https://www.interpol.int/en/content/download/590/file/Constitution%20of%20the%20ICPO-INTERPOL-EN.pdf.
[4] https://www.interpol.int/en/content/download/591/file/02%20E%20GEN%20REGULATIONS%2011%2012%2019_ok.pdf.

		Additional documents that make up INTERPOL's legal framework[5]
X	Other (summarize and provide copy of relevant portion)	Agency Service Standards, Network Connection Interface Service Agreements to support Infrastructure connectivity.

The mission of the USNCB as set forth in Title 28, Code of Federal Regulations, Section 0.34, is to facilitate international law enforcement cooperation as the United States representative to INTERPOL, the International Criminal Police Organization, on behalf of the Attorney General, pursuant to 22 U.S.C. 263a.

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, B, C and D	
Date of birth or age	X	C and D	
Place of birth	X	C and D	
Gender	X	C and D	
Race, ethnicity or citizenship	X	C and D	
Religion	X	C and D	
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	
Tax Identification Number (TIN)	X	C and D	
Driver's license	X	C and D	
Alien registration number	X	C and D	
Passport number	X	C and D	
Mother's maiden name	X	C and D	

[5] More information on the documents that make up INTERPOL's legal framework can be found here: https://www.interpol.int/en/Who-we-are/Legal-framework/Legal-documents.

(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
Vehicle identifiers	X	C and D	
Personal mailing address	X	C and D	
Personal e-mail address	X	C and D	
Personal phone number	X	C and D	
Medical records number	X	C and D	
Medical notes or other medical or health information	X	C and D	
Financial account information	X	C and D	
Applicant information	X	C and D	
Education records	X	C and D	
Military status or other information	X	C and D	
Employment status, history, or similar information	X	A, C and D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	
Certificates	X	C and D	
Legal documents	X	C and D	
Device identifiers, e.g., mobile devices	X	C and D	
Web uniform resource locator(s)	X	C and D	
Foreign activities	X	C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	
Juvenile criminal records information	X	C and D	
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	
Whistleblower, e.g., tip, complaint or referral	X	C and D	
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	C and D	
Location information, including continuous or intermittent location tracking capabilities	X	C and D	
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	
- **Video containing biometric data**			
- **Fingerprints**	X	C and D	
- **Palm prints**	X	C and D	
- **Iris image**	X	C and 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: 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
- **Dental profile**	X	C and D	
- **Voice recording/signatures**	X	C and D	
- **Scars, marks, tattoos**	X	C and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	C and D	
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	
- **User passwords/codes**	X	A and B	
- **IP address**	X	A and B	
- **Date/time of access**	X	A and B	
- **Queries run**	X	A and B	
- **Content of files accessed/reviewed**	X	A and B	
- **Contents of files**			
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	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Sharing with Foreign officials pursuant to the INTERPOL Rules on Processing Data (RPD).[6]					

[6]The INTERPOL Rules on the Processing of Data (RPD) lay down the general principles and rules governing all processing of data in the INTERPOL Information System (IIS). This includes provisions governing the quality, use, access, retention, dissemination, classification and security of the data processing in the IIS.

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
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	See above section 2.1
DOJ Components	X	X		See above section 2.1
Federal entities	X	X		See above section 2.1
State, local, tribal gov't entities	X			See above section 2.1
Public	X			In response to a Freedom of Information Act (FOIA), or other requests for government documents
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			In response to a FOIA, or other requests for government documents In response to Subpoenas or other court orders
Private sector	X			In response to a FOIA, or other requests for government documents
Foreign governments	X			See above section 2.1
Foreign entities	X			See above section 2.1 International Organizations – INTERPOL, Europol

https://www.interpol.int/content/download/5694/file/24%20E%20RPD%20UPDATE%207%2011%2019_ok.pdf

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.**
Other (specify): International Organizations – INTERPOL, Europol	X			

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.

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.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

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.

None. Individuals do not have the opportunity to voluntarily participate, consent to particular uses, or decline to provide information. With regard to ECE information maintained as a record in a system of records, the Attorney General has exempted the USNCB from the access, contest, and amendment provisions of the Privacy Act.

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.

Information in ECE is available to individuals only through appropriate requests made pursuant to the FOIA. With regard to ECE information maintained as a record in a system of records, the Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(1), (2), and (3), (e)(4)(G) and (H), (e)(5) and (8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), and (k)(2) and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and

(e) and are published in the Federal Register. *See* 28 CFR 16.103. The USNCB is exempt from subsection (e)(3) because supplying an individual with a statement of intended use of the requested information could compromise the existence of a confidential investigation, and may inhibit cooperation.

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): 31 Dec 2019** **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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: The only Privacy related POAM is to complete the Privacy Impact Assessment.**
	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:** Monitoring functions have been implemented and are conducted on a constant basis at the perimeter of the environment as well as within the internal network. The system security is tested and evaluated on a quarterly and annual basis in support of operational and regulatory requirements.
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:** Auditing functions have been implemented at both the network and application levels. All actions within the environment are tracked and reviewed for unusual activities.
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:** There is no additional training specific to ECE. All USNCB personnel who handle PII for 60 days or more at the USNCB are required on an annual basis to complete the Department of Justice's

	Office of Privacy and Civil Liberties (OPCL) mandatory privacy training course via LearnDOJ.

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?

ECE has a Federal Information Processing Standard (FIPS) 199 Security Categorization of Moderate. This categorization requires protection to safeguard data and information from unauthorized modification, and to ensure the organization's services are available to meet mission requirements. All data that resides within USNCB systems are protected by multiple layers of security controls and protection measures to include but not limited to access control devices and techniques, perimeter protection and detection technologies, viral and malware devices, encryption, enhanced authentication techniques, and physical security devices. A formal Certification and Accreditation (C&A) effort was completed that included a full risk assessment and final technical analysis that concluded that privacy data is adequately protected.

All data that resides within USNCB systems are protected by multiple layers of security controls and protection measures to include but not limited to access control devices and techniques, perimeter protection and detection technologies, viral and malware devices, encryption, enhanced authentication techniques, and physical security devices. In addition, all member countries of the INTERPOL organization agree to adhere to specific data handling and protection requirements as identified within the INTERPOL Constitution and Regulations, as referenced in Section 2.2, above. Additionally, the USNCB maintains MOUs with U.S. partner law enforcement organizations that specifically address authorization of these entities to access INTERPOL controlled data, as well as the appropriate handling and safeguarding of the data. Finally, all information provided to outside law enforcement entities, and humanitarian aid provided to internet service providers, is accompanied by the following Disclaimer to ensure information is properly handled and protected:

****
This message and any attachments contain sensitive law enforcement information that should be protected from unauthorized access and used only for law enforcement purposes. Any further dissemination of this message and any attachments is restricted to official law enforcement authorities for legitimate law enforcement purposes. Any other distribution of this information without the consent of the U.S.N.C.B.is prohibited.

In addition, as stated above, the ECE user community consists of USNCB investigative analysts, agents, contractors, and interns. The investigative analysts are permanent employees within the Department of Justice. The agents are detailed from participating U.S. state, local, federal and tribal law enforcement organizations as representatives of their respective organizations and provide investigative support to the USNCB. Only those individuals specifically authorized have access to the USNCB records. Access to USNCB records is given only to those individuals who require access to perform official duties. There are no outside users permitted access to ECE, including personnel from the larger DOJ community.

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.)

Case files closed as of April 5, 1982, and thereafter are disposed of as follows: The hard copy (paper record) will be retained on site at the USNCB for two years after closing. At the end of the two years post-closing, the hard copy (paper record) will be transferred to the Washington National Records Center for storage. The hard copy of the case file may be destroyed five years after transfer to the Washington National Records Center, for a total of seven years post-closing, if there has been no case activity. Information contained in electronic case files is comprised of the actual file (eg., .pdf, .doc, etc.) and meta tag data which describes the file content. While the actual file is stored by the government using an on-premise storage server, the meta tag data is stored within a database hosted in the government cloud. Both the actual files and their associated meta tag data will be stored for seven years, after which they will be removed seven years post-closing if there has been no case activity.

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:

System Name: INTERPOL-United States National Central Bureau (USNCB) Records System, JUSTICE/INTERPOL-001
75 FR 27821 (05-18-2010)
82 FR 24151, 158 (05-25-2017)

https://www.justice.gov/opcl/doj-systems-records#INTERPOL

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.***

USNCB employs a number of procedural and technical tools to identify and mitigate privacy risks. This includes working with users, employing policies, and deploying technology as described below.

Risk	Description	Mitigation
Improper collection	**Improperly collecting or keeping data that should not be kept.**	**Training, Proper limits by tools**
Improper Storage	**Improperly storing data on the USNCB system by failing to restrict access**	**System Architecture and data rules, Adhere to IPSG RDP**
Improper Use	**Improperly using data by USNCB team to include any USNCB users**	**Initial training to new users and annual training, Automated Rules**
Improper Release	**Improperly exposing data through email, reports, or conversation**	**Training users on expected behaviors and action. Deploy Email protections that scan for PII and freeze emails that appear to be violating protocol.**
Improper Response to issues	**When situation discovered, Activate procedures to mitigate**	**Training, coordination, testing/practice**

Mitigation of Privacy Risks

1. People
    a. All federal and contracted employees, and interns, are required to complete annual OPCL Privacy training.
    b. All USNCB team members, including detailees, interns, and federal and contracted employees, are required to complete annual CSAT training.
    c. All USNCB team members, including detailees, interns, and federal and contracted employees, are required to review and acknowledge application of the USNCB Rules of Behavior before being granted access to OA/Envoy.
    d. Users are reminded to use care when communicating with partners.
    e. Access to USNCB information is given only to those individuals who require access to perform official duties. There are no outside users permitted access to ECE, including personnel from the larger DOJ community.
2. Policies
    a. Training in the proper usage of ECE is provided as part of the job. As roles change or users move to new USNCB teams, access can be adjusted.

b. Usage patterns are tracked and reviewed for anomalous behavior.
c. Users are granted access to only the information applicable to their role.
d. USNCB collects only that data which is required to complete the tasks at hand.
e. USNCB follows both DOJ Privacy regulations with INTERPOL's Rules for Processing Data (RPD) and other governing rules.
f. When an USNCB employee departs the agency, appropriate measures are taken to deactivate the user access and accounts to USNCB information.
g. On an annual basis, the USNCB Information Technology Division performs user account validations to maintain appropriate active users' access and deactivate inactive users' access to USNCB information.

3. Technology
    a. Using the DOJ Identity Management solutions, USNCB controls who can access what information.
    b. Security defenses are shared with DOJ JSOC to ensure appropriate perimeter control and data content monitoring.
    c. Security Defenses are augmented by solutions deployed within USNCB, including additional firewalls and monitoring tools.

The techniques and tools described above are used to manage the risks as described below.