Office of Community Oriented Policing Services (COPS Office)

Privacy Impact Assessment for the COPS Office Resource Center

Issued by:
Melissa Fieri-Fetrow
COPS Office
Senior Component Official for Privacy

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: May 7, 2025

(May 2022 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 Office of Community Oriented Policing Services (COPS Office) Resource Center (RC) serves as a centralized repository for digital and physical resources developed by the COPS Office.

The purpose of the COPS Office RC is to provide a mechanism for the nation's state, local, territorial, and tribal law enforcement agencies and the communities they serve to access a variety of free resources, including publications, brochures, flash drives, and toolkits developed by the COPS Office.

Viewing the catalog does not require a user to sign-in, and no PII is requested or collected if a customer only wishes to view or download a resource online from the COPS Office RC. If the user wishes to place an order for physical copies of material, the individual or corporation is required to create an account. The COPS Office RC collects username, first name, last name, email address and password to create an account. The collected information is stored in the COPS Office RC system database. Once the user adds the desired items to the cart, the user is required to enter shipping information to have the item(s) shipped. The PII collected is organization/individual's name, email address, shipping addresses and phone number. The shipping information is required each time the user wishes to order COPS Office resources, and the shipping information collected is stored with the order in the COPS Office RC system database. This information is stored and collected to allow the COPS Office to fulfill order requests of COPS Office resources. No artificial intelligence or machine learning will be used to process COPS Office resource orders.

Access to PII information stored within the COPS Office RC is limited to COPS Office internal federal and contractor staff and to external warehouse contract staff who have the role and permission-based access to manage the inventory and to process orders in the system.

This Privacy Impact Assessment was conducted to determine whether there are privacy risks associated with the COPS Office RC and, if so, to evaluate ways to reduce those risks.

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 COPS Office is the component of the U.S. Department of Justice (Department) responsible for advancing the practice of community policing by the nation's state, local, territorial, and tribal law enforcement agencies through information and grant resources. The COPS Office information resources cover a wide range of community policing topics such as school and campus safety, violent crime, and officer safety and wellness.

The COPS Office RC supports the COPS Office mission of advancing community policing by providing a mechanism to promote a variety of free resources, including publications, brochures, flash drives, and toolkits and providing the nation's state, local, territorial, and tribal law enforcement agencies and the communities they serve with access to these resources and the ability to share the knowledge, research and promising practices in addressing a wide range of topics advancing community policing.

The COPS Office internal federal and contract staff manage system access, roles, and permissions. The external warehouse contractor handles fulfillment of COPS Office resource orders through role and permissions-based access. Information accessible to the external warehouse contractor allows the COPS Office to fulfill shipment requests of COPS Office resources received in the system. These requests support the COPS Office mission to advance the practice of community policing nationwide.

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
Statute	The Violent Crime Control and Law Enforcement Act of 1994 (Pub. L. 103-322) and 34 U.S.C. §§ 10381 – 10389
Executive Order	
Federal regulation	
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, B, C, D	Name of individual/organization requesting publications
Date of birth or age			
Place of birth			
Sex			
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, B, C, D	Addresses of individuals/organization requesting publications
Personal e-mail address	X	A, B, C, D	Addresses of individuals/organization requesting publications
Personal phone number	X	A, B, C, D	Phone numbers of individuals/organizations requesting publications
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			
Web uniform resource locator(s)			

(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
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			
Biometric data:			
- **Photographs or photographic identifiers**			
- **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, B, C and D	System audit related Information, e.g., user ID of COPS Office employees and contractors and members of the public
- **User passwords/codes**	X	A, B, C, and D	System audit related information, e.g., passwords of COPS Office employees and contractors and members of the public
- **IP address**	X	A, B, C, and D	System audit related information, e.g., IP address of COPS Office employees and contractors and members of the public

- **Date/time of access**	X	A, B, C and D	System audit related information, e.g., date/time of access of COPS Office employees and contractors and members of the public
- **Queries run**			No queries are being run on the system
- **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	X
Phone		Email			
Other (specify):					

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

Non-government sources:					
Members of the public	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	Information is only shared with individuals with role-based access to the system based on a need to know.
DOJ Components				
Federal entities				
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.

Information collected through the COPS Office RC system will not be released to the public for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

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

The COPS Office will notify individuals directly with a Privacy Act §552a(e)(3) notice. Records maintained on requests to receive a copy of resources available via the COPS Office RC are covered by SORN JUSTICE/COPS-002, COPS Online Ordering System, 77 FR 28898 (5-16-2012); 82 FR 24151, 155 (5-25-2017).

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.

Individuals must provide their name, phone number, email and mailing addresses only if they would like to receive a copy of a COPS Office resource via mail or email.

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.

Records maintained for the purpose of providing resources available via the COPS Office RC can be accessed or amended, in accordance with DOJ regulations, and in accordance with SORN JUSTICE/COPS-002, COPS Online Ordering System, 77 FR 28898 (5-16-2012); 82 FR 24151, 155 (5-25-2017).

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):** The COPS Office Public Website houses the COPS Office RC, ATO has been successfully renewed from 12/22/24 – 12/22/25. **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:** **After further research no items are deemed sensitive and cannot impose a risk to the COPS Component. No items will be created at this time.**
	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: N/A
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** COPS Office RC, it is a central hub database that serves as a digital library online ordering system comprised of community policing topics, best practices, and other publications within law enforcement that address crime and other disorderly challenges that the state and local agencies face. Users can login in with their account or create an account to access this material. Because the COPS Office RC inherits COPS Office Public Website controls and because of the

	limited, non-sensitive personal information collected, the system Security Categorization is Low.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The COPS Office uses the listed monitoring tools, for evaluation, testing and remediation along with information system audit logs, agency mandated IRP, and ISCP tabletop Exercises: Security Posture Overall Risk Assessment Vulnerability Management Risk Assessment Configuration Management Risk Assessment Software Management Risk Assessment General User PIV Compliance Vulnerability - VPR Risk Assessment Vulnerability - Patch Risk Assessment Vulnerability - Vulnerability Risk Assessment Software - Unsupported Software Risk Assessment Software - Antivirus Risk Assessment
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:** COPS Office auditing procedures for role-based access include: (1) periodic account reviews are conducted for all system accounts (regardless of role) at least every 90 days to ensure inactive accounts are identified and to ensure that users have the appropriate access; (2) authorized users must authenticate their COPS Office account passwords every 90 days; (3) system administrators annually review all user accounts and validate them; and (4) system administrators review audit checklist and user info log files collected by the system daily to resolve identified issues such as event alerts, security errors, and unauthorized use alerts.
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**. Contractors that have access to COPS Office RC are subject Federal Acquisition Regulation (FAR) clauses 52.224-1 to 52.224-2 (Privacy Act provisions), which are included in their - ITSS-5 contract, which includes standard privacy terms in DOJ-02 and security terms in DOJ-05.
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:** Each FY COPS federal staff and contractors are required to complete CSAT and OPCL privacy training that addresses employee responsibilities regarding the handling of personally identifiable information (PII) and privacy safeguards.

	ROB: Rules of behavior forms are used to help maintain security and acceptable level of risk for DOJ systems and applications. Paper and/or electronic records of account management actions are being performed in accordance with DOJ and system specific procedures.

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?

Several key preventative measures are in place to maintain security and privacy within the COPS Office RC. To reduce the risk of unauthorized access and disclosure of information, access controls are being enforced at the user and application level. Requestors can only input contact information into the data fields. Role-Based Access Control (RBAC) is used to restrict access and what a user can view based on a user's role to complete their job duty. This control strengthens COPS security posture and improves overall privacy compliance. Periodic account reviews are conducted for all system accounts (regardless of role) at least every 90 days to ensure inactive accounts are identified and to ensure that users have the appropriate access. Authorized users must authenticate their COPS Office account passwords every 90 days. All login activity is monitored through audit logs to detect unusual behavior. To limit what information is being requested and provided, validation rules are set to restrict data input for each data field to ensure only a requester's organization/individual's name, email address, shipping addresses and phone number are collected. This security measure will prevent unnecessary sensitive information from being requested or submitted.

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 COPS Office RC records are retained and disposed of in accordance with records retention schedules approved by the National Archives and Records Administration. NARA's General Records Schedule (GRS) 4.2. Information will only be used to fulfill order requests.

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/COPS-002, COPS Online Ordering System, 77 FR 28898 (5-16-2012); 82 FR 24151, 155 (5-25-2017).

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.***

A. Privacy risk associated with information being collected

The COPS Office RC does not collect PII if users only view or download a resource. In addition, the system limits the risk of over collection or misuse of information by only requiring the necessary PII data types to have the requested resources shipped. COPS Office RC data is encrypted from to end-end, databases use an encryption mechanism aligned with NIST Framework, encrypting data at rest and data in transit.

B. Privacy risk associated with information being used

COPS federal staff and contractors with authorized access have limited functionality based on their roles, implementing least privilege functionally to perform tasks in the system. Information will only be used to process or fulfill online ordering requirements and only authorized users with sufficient roles will be able to view user information.

COPS federal staff and contractors receive mandatory (CSAT and OPCL privacy) training and ROB forms before gaining access to the system, adhering to DOJ security and privacy best practices.

The COPS Office will inform individuals about the collection, use, sharing or other processing of their PII with a Privacy Act §552a(e)(3) notice. Information collected for requests to receive a copy of resources available via the COPS Office RC are covered by COPS Online Ordering System 77 FR 28898 (5-16-2012); 82 FR 24151, 155 (5-25-2017).

C. Privacy risk associated with dissemination of information

To minimize privacy risks associated with dissemination of information, PII is not shared or accessed by users that do not have the appropriate permissions. Authorized COPS federal staff and contractors are granted the least amount of access necessary using role-based permissions, and they are required to use unique, secure login credentials. All login activity is monitored through audit logs to detect unusual behavior. Finally, COPS federal staff and contractors are required to sign and comply with the Rules of Behavior. Access is revoked immediately when the contract is terminated, and/or employment ends.

D. Security, physical and administrative controls over information

Information collected is stored in the COPS Office RC database, and databases are encrypted at rest and in transit using a secure encryption standard, Advance Encryption Standard-256 (AES), one of the most secure encryptions standards in hardware and software. Security administrative control used over information is Role-Based Access Control (RBAC) which restricts access and what a user can view based on the user's role to complete their job duty. This control strengthens COPS security posture and improves overall privacy compliance. Periodic account reviews are conducted for all system accounts (regardless of role) at least every 90 days to ensure inactive accounts are identified and to ensure that users have the appropriate access. Authorized users must authenticate their COPS Office account passwords every 90 days.