U.S. Department of Justice
Office of Professional Responsibility

Privacy Impact Assessment
for the
OPR APPS (OAPPS)

Issued by:
Margaret McCarty

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

Date approved: June 8, 2020

Blank Page

EXECUTIVE SUMMARY

The Office of Professional Responsibility (OPR) has jurisdiction to investigate allegations of professional misconduct against Department of Justice attorneys that relate to the exercise of their authority to investigate, litigate, or provide legal advice, including allegations of professional misconduct against Department immigration judges. OPR also has jurisdiction to investigate allegations of misconduct against Department law enforcement personnel that relate to allegations of attorney misconduct within the jurisdiction of OPR. In addition, OPR investigates allegations of reprisal against current or former FBI employees or applicants for making protected disclosures.

OPRNET APPS (OAPPS) is a cluster of the Department of Justice's Justice Management Division (JMD)-operated Microsoft Windows-based servers, hosted in the Azure cloud service. The OAPPS system provides investigative matter workflow management and document management application to support the processing of investigations performed by OPR staff.

This Privacy Impact Assessment is being conducted because the OAPPS system collects, maintains, and disseminates personally identifiable information (PII), to include as names, addresses, phone numbers, e-mail addresses, work information, titles, and Social Security Numbers, of complainants, subjects, witnesses, and other individuals involved in OPR investigatory matters.

Section 1: Description of the Information System

OPRNET APPS is a major application system that operates on multiple Microsoft Windows Servers with Microsoft SQL database servers, hosted on the Department of Justice-managed Microsoft Azure Cloud service. The workflow for processing OPR matters requires running and storing information on the customized case management application and the document and record management application, both provided by contractors.

In the past, a complainant would submit complaints to OPR by either sending a facsimile or through physical document delivery by either U.S. Postal Service or other express delivery services. Each complaint was read and evaluated for validity by an OPR staff member and the information would then be entered into the OAPPS system. Using the information stored in the system, the complaint would be adjudicated by the OPR analysts or OPR attorneys, depending on the gravity of the complaint.

The complainant would be required to provide their name and contact information, as well as information regarding the subjects or witnesses involved with the complaint. Information such as names, addresses, phone numbers, titles, positions, work addresses, email addresses and other information is requested in order for the complaint to be processed.

OPR is in the process of introducing a new method for complainants to submit complaints to the office. The Complaint Intake Web-form (CIW) will be placed on OPR's public-facing website on www.justice.gov, where anyone can file a complaint to OPR by filling out the form with the necessary

information.

The CIW will request the same information required for a paper-based process in order for OPR to process the complaint. Information submitted by the complainant, through the CIW, will be sent through the DOJ's email network to a designated OPR email address that is accessible by a select few OPR staff, who are assigned to the intake process, which is explained in more detail below. CIW complaints receive the same review process as a complaints submitted in paper form. OPR worked with OPCL to draft a Privacy Act statement under 5 U.S.C. 552a(e)(3)to include on the web form, due the form collecting information from the public.

OPR also processes vetting requests from every component of the Department of Justice. When Department attorneys, law enforcement officers, paralegals or other legal staff are being processed for an award, retirement, presidential appointment, promotion or background investigation, the component representative sends vetting requests to OPR to verify if there were any allegations made against the person and if any negative findings are listed in OAPPS.

In the vetting process, the components submit information on the staff being vetted, including names, offices, titles, positions, date of birth and last four digits of Social Security Numbers, which are used to distinguish people with the same name. Vetting requests on average will top 2500 individuals per year. Each requestor will receive an individualized response after OPR has completed its verification processes.

The information stored in the OAPPS system is used to generate reports to the Attorney General, the Deputy Attorney General, and the head of the Executive Office for United States Attorneys (EOUSA) for review.

Quarterly reports are sent to the Attorney General, the Deputy Attorney General, and the head of EOUSA with the work that OPR has performed in the past quarter. This report contains personally identifiable information of the subjects, complainants, and witnesses, for each matter.

An Annual Report is created, after each fiscal year, that provides an overview of OPR's work during the past year. The annual reports do not contain any personally identifiable information. After the review and approval of the report by the Attorney General, the report is published on OPR's website as a public record. Vetting requests are not included in the reports.

Access to the data on OAPPS servers is limited via the corresponding case management and document management client applications installed on the OPR workstations. Both case management and document management applications use access control lists, which the OPR's Information Technology Specialist manages, to limit users' connection to the servers. Since the migration to the Department's Azure Cloud infrastructure, JMD's Windows Service team is responsible for maintenance, backup, and upkeep of the Azure servers. The Windows Service team and OPR's Information Technology Specialist have full access to the servers.

The information is kept in the system after the completion of the investigation and closure of the

complaint according to the OPR's Records Management schedule. The information is then purged from the system after the proper retention time has elapsed.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Distinguishing features/Biometrics
Other distinguishing features/biometrics (specify):

System admin/audit data					
User ID		Date/time of access		ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)

The Complaint Intake Web-form contains one or more free text fields for complainants to describe their allegations. While the form only seeks information relevant to the complaint, a complainant may include information not relevant or necessary for the complaint that may include additional personally identifiable information of the complainant, witnesses, or others, e.g., age or medical information. Also, during the course of an investigation, an investigator may collect additional PII that appears relevant initially but later turns out not to be relevant but nonetheless needs to be retained to comply with record retention requirements, as stated below.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign			
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OPR is an internal investigative office and does not actively seek or collect personally identifiable information from the general public. All information contained in the OAPPS system is collected by voluntary submission from complainants as part of their complaint process. The PII of additional people such as subjects and witnesses is collected, as needed, as part of the investigation process. There is a risk of collecting more information than is required to adjudicate a complaint. This risk was mitigated by creating the CIW and restricting questions on the form to only those required to fulfill OPR's mission.

Direct access to the database and PII stored on the OAPPS system is restricted to OPR staff only, through the use of the respective client applications. However, JMD's Windows Service Group performs the management of the OAPPS system server infrastructure and those with Administrator privileges also have access to the server.

There is potential risk involved with users other than OPR staff accessing the server. OPR has determined that this risk is acceptable because DOJ staff who have access to OAPPS servers are qualified and vetted DOJ contractors and staff subject to requirements by contract or policy to only use DOJ information as specifically authorized, receive privacy and information security training, and have access to all other DOJ components' servers, including the offices for the Attorney General and the Deputy Attorney General.

There is a risk that the information could be shared in a manner not required to facilitate OPR's statutory functions or otherwise not according to law or DOJ policy. This is mitigated through a variety of controls, including by requiring OPR staff to take annual mandatory privacy and information security training, which detail the circumstances under which PII may be shared.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities

	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

OPR's mission is to investigate allegations of professional misconduct involving Department attorneys and law enforcement officers in Department-related legal matters. OPR will use the PII to locate and identify the subjects, sources, witnesses, and the complainants, and to investigate the allegations. Without this PII, OPR could not accomplish its mission.

OPR only collects information from persons involved in a specific OPR matter. OPR does not solicit and collect information from DOJ staff or from the public who are not involved in a matter.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
x	Statute	44 U.S.C. 3101 et seq.
	Executive Order	
x	Federal Regulation	28 C.F.R. 0.39 et seq.
	Memorandum of Understanding/agreement	
x	Other (summarize and provide copy of relevant portion)	Attorney General Order No. 833–79

3.4 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.)

Office of Professional Responsibility has an approved records retention schedule by the Department of Justice Office of Records Management Program (ORMP) and the National Archives Records Administration (NARA).

OPR processed matters are given one of four matter classifications. The length of their information retention varies depending on the type of matter classification.

- Correspondence Matters: 5 years from closed date
- Inquiry Matters: 5 years from closed date
- Investigation Matters: 15 years from closed date
- Historical Matters: Permanent records. After 15 years from closed dated, the data related to the matter, including documents, are sent to NARA for permanent storage and the data is purged from OAPPS system.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

OPR staff is required to complete annual privacy training that details how to properly create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII in carrying out authorized Department functions.

OPR accomplishes PII minimization by scoping the CIW appropriately and disposes of records in accordance with the above-detailed records retention schedules. OPR also seeks to collect PII to the greatest extent practicable from the individual to whom the information pertains.

OPR must also complete information security awareness training. OPR also has an Information Technology Specialist on staff to handle any IT problems, and the OPR Security Program Manager who provides guidance and tips throughout the year in safeguarding and handling sensitive information.

All workstations used by OPR staff are centrally managed and kept up-to-date by JMD security staff. Technical security management of viruses, malware and other security problem detections are handled through JMD.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components	X			

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Federal entities	X			
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments				No Foreign Government Access
Foreign entities				No access to foreign entities
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

OPR information is disclosed on a very limited basis and only after extremely rigid review and authorization. OPR reports of investigation are disclosed only after extensive review internally and Office of the Deputy Attorney General's (ODAG) approval. All OPR staff receive training, as noted above, and are repeatedly advised about the confidentiality of the information and to not disclose information without review and approval.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
x	Yes, notice is provided by other means.	Specify how: All subjects of an investigation are provided written notice of the investigation regarding their conduct. The CIW will also contain a Privacy Act statement that is provided in Section 5.4
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

x	Yes, individuals have the opportunity to decline to provide information.	Specify how: Complainants, witnesses or subjects of OPR investigations who are not currently employed by the Department are not required to provide information.
X	No, individuals do not have the opportunity to decline to provide information.	Specify how: Department employees are generally required to cooperate with OPR and provide information relevant to the allegation of misconduct. However, OPR only seeks information from the individual that is relevant to the specific allegations in the investigation. All PII is kept confidential and is not disclosed outside the Department without authority from the ODAG.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: As noted, the information that OPR collects as part of an investigation into misconduct is made clear to Department attorneys. The majority of the information OPR collects relates to the attorney's duties and actions as Department employees. The exact use of that information for conducting an investigation is made clear to the individual. No other use is made of the information.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

OPR provides notice to the Department attorney regarding how the information that is provided to it will be used during the investigation. The subject attorney is provided written notice of the investigation and asked to respond to questions and provide information about the allegations. Most of this information relates to the attorney's duties and position with the Department.

The CIW will include a Privacy Act Statement to provide clear and conspicuous notice, providing transparency and allowing individuals to understand how their information will be handled. The Privacy Act is as follows:

PRIVACY ACT STATEMENT

The authority by which information is collected on this website form is 44 U.S.C. 3101, 28 CFR 0.39, and Attorney General Order No. 833-79. Your disclosure of information on this form to the Department of Justice, Office of Professional Responsibility ("OPR") is voluntary. If you do not complete all or some information fields in this form, however, the OPR may not be able to effectively respond to your feedback.

The principal purpose for collecting and maintaining the information on this website form is to control, track, respond to, and maintain correspondence that is received, originated or referred to OPR regarding the resolution of allegations of professional misconduct made against Department employees, FBI Whistleblower complaints, and to advise complainants of the status of investigations and the results. Information is also maintained for purposes of making a determination concerning the possible referral of certain allegations of professional misconduct made against non-Department attorneys to the appropriate licensing authorities. In addition to those disclosures generally permitted by the Privacy Act, all or a portion of this information may be disclosed as a routine use, which include, but are not limited to, disclosures : to any civil or criminal law enforcement authority or other appropriate agency where a record, either alone or in conjunction with other information indicates a violation or potential violation of law; to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to the corresponding system of records; to any person or entity that OPR has reason to believe possesses information regarding a matter within the jurisdiction of OPR, to the extent deemed to be necessary by OPR, in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity; or to such recipients and under such circumstances and procedures as are mandated by federal statute or treaty. The full list of routine uses for this correspondence can be found in the System of Records Notice titled, JUSTICE/OPR-001, "Office of Professional Responsibility Record Index for the Department of Justice," 76 Fed. Reg. 66752 (10-27-2011); 82 Fed. Reg. 24151, 161 (5-21-2017); JUSTICE/JMD-023, "Federal Bureau of Investigation Whistleblower Case Files," 70 Fed. Reg. 53253.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: JMD is the system owner of the boundary containing OAPPS, namely the Email and Collaboration Services (ECS). ECS last received an Authorization to Operate in October 2019. The Privacy Impact Assessment for ECS can be found here: https://www.justice.gov/ECS_PIA/download If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

OAPPS information is restricted to OPR staff with access to OPR workstations with the client applications configured. Other Department users in DOJ will not have access to the application configuration.

A second layer of security controls is provided from the internal access control list that is used by the document management server and case management server. Even if a user has the application configuration, the corresponding authorized user account must exist in OAPPS system to be granted access to the data.

The OAPPS servers are created and managed by the JMD's Windows Service team. OPR relies on JMD's customary controls to prevent or to detect unauthorized administrator level access to the server by the members of the JMD Windows Service team. This risk has been deemed acceptable by OPR.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

x	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: JUSTICE-OPR-001, Office of Professional Responsibility Record Index, 76 Fed. Reg. 66752 (Oct. 27, 2011)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

U.S. citizen and Lawful Permanent Resident information in the system is retrieved by personal identifiers.