Department of Justice
Office of the Inspector General

Privacy Impact Assessment
for the
Justice OIG Survey System (JOSS)

Issued by:
Jonathan M. Malis
Senior Component Official for Privacy

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

Date approved: July 5, 2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Justice OIG Survey System (JOSS) is used by the OIG to distribute customized surveys within the OIG, to the Department of Justice (DOJ or Department) components, and to external parties. The system is owned, managed, and maintained by OIG Office of Data Analytics (ODA). Once users receive a Qualtrics account they can access survey templates and form questions to build customized surveys that can be distributed electronically through the internet and via email.

JOSS is the Office of the Inspector General's (OIG) instance of Qualtrics XM, a Federal Risk and Management Program (FedRAMP) Moderate Software as a Service (SaaS) Government Community Cloud (GCC) system. The FedRAMP Joint Authorization Board (JAB) issued Qualtrics XM SaaS a Provisional Authority to Operate (P-ATO) for federal government agency use.

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 OIG uses JOSS to conduct surveys for two main purposes: first, to collect information from OIG employees (internal surveys) and second, as part of an audit, evaluation, or review of Department components, grantees, employees, or those affected by the actions of the Department (external surveys). Internal surveys are used to collect OIG employee feedback to provide context and information on the operation of the OIG. External surveys are issued by the OIG but completed by individuals outside the OIG to gather information that informs the OIG's official work, such as audits, evaluations, or reviews. These survey results can be published as part of a public report or used internally to inform OIG work.

Information in JOSS will be collected from two distinct groups. Users are the OIG employees that log in to the system to create, disseminate, and analyze surveys. Respondents are those people who provide responses to the surveys, whether OIG employees, DOJ employees, or members of the public.

Users will have log in information and access to any information related to a survey they are working on collected by the system. The system will also house contact information for anyone who might take a survey. Contact information will either be uploaded by the user or come through a connection to the DOJ address book in Outlook.

Respondents will provide responses to various questions including, in some cases, demographic information such as employment, race, gender, or age. Other survey questions generally ask about individual perceptions, such as a respondent's thoughts or observations on a topic.

Only DOJ OIG employees can be users with access to the data within JOSS. Respondents to surveys will not have user access to JOSS but will be provided with a link to access a form to

complete the survey. A JOSS account is not required to respond to a survey. Currently, no more than three OIG users have administrative privileges for JOSS. These users, called 'Brand Administrators,' are assigned to manage security configuration settings in Qualtrics.

The system is hosted by Qualtrics SaaS with data storage provided by the vendor. Specific customer security and privacy controls are the responsibility of OIG for implementation and continuous monitoring. OIG contractors do not currently have access to the Qualtrics system.

Qualtrics employees have limited access to certain information about the OIG's usage of JOSS, including user profiles, response counts, number of open projects, and recent requests for support. Qualtrics does not have access to any data that is collected by the OIG through the use of JOSS (e.g., directories, responses, analysis etc.). Qualtrics has strict guidelines around what it can and cannot do with customer data.

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	5 U.S.C. § 406(a)(3) 5 U.S.C. § 406(a)(9) 5 U.S.C. § 406(j)(2) 5 U.S.C. § 404(a)(1) and 404(a)(3)
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.

The information in the table below captures the expected types of information that will be included; however, it is not exhaustive of the information that may be processed. All DOJ (including OIG) users' names and any names used as part of a contact list for disseminating surveys may be collected, maintained or used by Qualtrics, including DOJ grantees as "public"

respondents to surveys. Respondents to surveys receive a link to complete the survey; respondents do not have access to the system.

Information can also include any demographic data provided by respondents to a survey.

For system admin/audit data, this is only for DOJ / OIG federal employees but can include username, date/time of access, and audit trail of work performed for OIG users. Ex. OIG User ID would be captured; passwords are not used or captured for OIG use. Access is via Federated or Multifactor Authentication and Single Sign On (SSO).

(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	See 3.1 above
Date of birth or age	X	A, B, C, D	See 3.1 above
Place of birth	X	A, B, C, D	See 3.1 above
Gender	X	A, B, C, D	See 3.1 above
Race, ethnicity, or citizenship	X	A, B, C, D	See 3.1 above
Religion	X	A, B, C, D	See 3.1 above
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			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records	X	A, B, C, D	See 3.1 above
Military status or other information			
Employment status, history, or similar information	X	A, B, C, D	See 3.1 above
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	See 3.1 above
- **User passwords/codes**			
- **IP address**	X	A	See 3.1 above
- **Date/time of access**	X	A	See 3.1 above

(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
- **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	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	
State, local, tribal		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		Private sector	
Commercial data brokers					
Other (specify): Note: members of the public include only DOJ grantees.					

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	Only OIG administrators of the system will have access, along with access granted to DOJ/OIG survey creators on an as needed basis.
DOJ Components	X			
Federal entities				
State, local, tribal gov't entities				
Public	X			Surveys may be sent to public DOJ Grantee respondents in the form of a link, however respondents alone do not have access to the system. No other public respondents will be issued surveys.
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.

N/A

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.

At the beginning of the survey, respondents will be informed of the applicable statutes and the

application as it relates to confidentiality of responses. Thus, respondents will be informed of how their data will be used before they provide any response. Respondents will also be reminded that the survey is voluntary.

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.

Respondents may elect not to respond to the survey after reading the notice explaining how their data will be used and being informed that the response is voluntary. It should be noted that the majority of surveys will be anonymized, unless specifically explained to the respondents otherwise.

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.

For each survey, OIG will indicate the point of contact associated with the survey in case any respondent would like to follow up on their response. The survey results will be subject to the OIG's normal Freedom of Information Act (FOIA) process.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO anticipated in June 2023, once privacy documentation is complete. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:

X	**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:** The DOJ OIG JOSS system is identified as a Moderate categorization system based on FIPS 199 information types, as documented in the system security and privacy plan.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The DOJ OIG JOSS system applicable and hybrid (shared with the Qualtrics XM vendor) security controls are implemented per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 and the DOJ Cybersecurity Control Standards. These controls have been documented in the System Security Plan (SSP) and System Security and Privacy Plan (SSPP). The controls have been evaluated and assessed, with the outcome documented in the Security Assessment Report (SAR) and Security and Privacy Assessment Report (SPAR).
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:** OIG ODA Brand Administrators review the audit log activity at least weekly, however, Brand Administrators can also view logs in real time. Only a limited number of OIG users have access to the system. The OIG procedure for reviewing audit logs will be reviewed and updated annually. The JOSS system applicable and hybrid controls implemented per NIST SP 800-53 Revision 5 and tested for initial ATO. After the ATO is received, the system is assessed annually by referencing a pre-defined set of core controls that are selected by the Department of Justice (DOJ) every fiscal year; the outcome of the assessment, including any controls that are Other Than Satisfied (OTS), are documented in an annual SAR. The SAR is distributed to the System Owner and Authorizing Official.
	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. DOJ OIG Contractors are not anticipated to access the system.
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:** OIG JOSS administrators will provide training, including any training from the vendor as applicable, with DOJ OIG employees who need to access the system.

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

Access is granted to the system by OIG Office of Data Analytics (ODA) JOSS administrators to a limited set of DOJ/OIG staff as needed to create surveys; once surveys have been processed, the survey creators' access is removed. Only OIG administrators and a limited number of ODA

team members will have permanent access to the system.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Information will be retained in accordance with the OIG records retention schedules for which the data was collected. This varies by division and includes:

- DOJ OIG Records Schedule (N1-060-10-17) for Audits, Evaluations, Inspections, Investigations, and Special Rev, May 20, 2011;
- DOJ OIG Schedule (DAA-0060-2012-0011) for Front Office, Semiannual reports, and other OIG Publications, June 10, 2013; and
- DOJ OIG Schedule (N1-060-09-024) for OGC programs and operations, including legal opinions and litigation case files.

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:

DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, Last published in full at 66 Fed. Reg. 29992 (June 4, 2001). The link to the DOJ-003 SORN is available from the following site location: https://www.justice.gov/opcl/doj-systems-records#doj or directly at https://www.govinfo.gov/content/pkg/FR-2001-06-04/pdf/01-13860.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?

The following privacy risks are associated with the collection, use, access, dissemination, and maintenance of the system's information:

- Unauthorized disclosure of OIG and DOJ components' business contact information. To mitigate the risk, the system will be synchronized with DOJ's Microsoft Exchange/Outlook directory for DOJ contact information for DOJ components and OIG.
- Loss of data and/or lack of data integrity of OIG and DOJ staff business contact information. To mitigate the risk, the system will be synchronized with DOJ's Microsoft Exchange/Outlook directory for DOJ contact information for DOJ components and OIG to ensure accurate information. Additionally, only ITD administrators will have the ability to implement this synchronization activity with the Exchange/Outlook directory; no other OIG users will have this access.
- Lack of Availability to OIG and DOJ staff business contact information. To mitigate the risk, the system will be synchronized with OIG's Active Directory nightly for the most up to date user account information for OIG users with access to the system. Additionally, only ITD administrators will have the ability to implement this synchronization activity.

The list below also provides additional details on how the risks are being mitigated:

1) Access to the system by OIG employees will be for a limited duration, to perform work on surveys, with the exception of permanent access provisioned to OIG brand or system administrators.
2) Survey data entered in the system is for a limited duration and will be removed from the system when no longer needed per record retention policy.
3) Public respondents are limited to DOJ Grantees; data submitted is anonymous and not identifiable to an individual unless they voluntarily provide that information.
4) Brand administrators and the Software as a Service vendor are not permitted to access the data in surveys by respondents. User accounts are separate for privileged users (administrators) and non-privileged users (e.g., OIG survey creators).