Environment and Natural Resources Division

Privacy Impact Assessment
for Qualtrics

Issued by:
Joseph M. Groves, Senior Component for Privacy

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

Date approved: [June 13, 2023]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Environment and Natural Resources Division (ENRD) is a core litigating component of the U.S. Department of Justice. Our mission is to enforce the Nation's civil and criminal environmental laws, including the Clean Air Act, Clean Water Act, and hazardous waste laws. Our mission also involves the protection of the Nation's natural resources and handling cases relating to tribal rights and resources. The Division's efforts result in significant public health and other direct benefits to the American people through the reduction of pollution across the Nation and the protection of important natural resources. The Division participates in criminal litigation to protect our nation's ecological and wildlife resources and internationally protected species, ensure the humane treatment of captive, farmed, and companion animals, protect the lives and the health of workers, and find justice for victims of environmental crime. It uses civil judicial actions to enforce most of the Nation's environmental laws like the cleanup of hazardous substance disposal/treatment sites; the pollution of the nation's surface waters; the pollution of the air we breathe; the integrity of our drinking water; the ongoing management of hazardous wastes and used oil; the regulation of chemical substances and mixtures which present a risk to human health and the environment; the disclosure of lead-based paint hazards; emergency planning for, and notification of, releases of extremely hazardous substances; and the protection of natural resources in national parks and marine sanctuaries.

It also represents the United States government and the interests of its citizens in affirmative civil and defensive civil litigation, defending pollution control laws, recovering costs for Superfund site clean-up, and representing federal agencies accused of being in violation of pollution control statutes. ENRD also litigates to protect lands held in trust for tribes and individual Indian lands, as well as the rights and resources associated with those lands, as well as defend challenges to decisions made by the Secretary of the Interior on behalf of tribes. Another function of ENRD is to acquire real estate by direct condemnation for Congressionally authorized public uses, like national parks, military bases, and federal courthouses. ENRD coordinates responses to legislative proposals and Congressional requests; prepares for appearances of Division witnesses before Congressional committees; and drafts legislative proposals in connection with the Division's work. ENRD facilitates initiatives on legal issues affecting minority and low-income communities that are disproportionately affected by environmental burdens and collaborates with communities to develop innovative projects to rectify environmental justice challenges. ENRD also conducts internal employee, DOJ employee, and international legal training and conducts human resources, financial, IT, customer service, and other administrative functions.

To support these litigation, policy, and administrative functions, ENRD needs to collect data from individuals. When face-to-face interviews or meetings are not feasible, the current solution is to email necessary information to the legal team. Email is not a secure protocol and leaves sensitive information – for the individual and the legal team – at risk. To mitigate potential data hacks and the mishandling of sensitive information, ENRD has procured and utilized Qualtrics, as a third-party "digital service," as defined by Office of Management and Budget (OMB) Memorandum M-17-06[1]. Qualtrics is a FedRAMP Moderate authorized, cloud-based digital survey service. Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with FISMA, OMB Circular A-130, and FedRAMP policy. Qualtrics is a cloud-based, on-line survey solution and used throughout government to collect individual feedback and analyze results. Qualtrics uses electronic

[1] .See OMB Memorandum 17-06, 3, available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-06.pdf ("digital services are defined . . . as online information resources or services" that "provide government information or services to the public or a specific user group across a variety of delivery platforms and devices and support the proper performance of an agency function."); see also id. at 3, n. 4 ("Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media")

forms to provide survey questions in English and other languages as needed and collects electronic results. Data is securely housed in its secure, cloud storage for processing, analysis, and export by permitted ENRD staff.

Qualtrics will be used to collect data from employees and the public. The general types of information collected, maintained, used, and/or disseminated through Qualtrics for the employee examples include but are not limited to: employee name; position; supervisory/non-supervisory; race, gender and age demographics; length of employment; feedback on management and team performance, impressions of workplace and engagement; training course attended; preferences for meeting times and locations; day and time of select appointments; preference and feedback on design materials. The general types of information collected from the public and maintained, used, and/or disseminated via Qualtrics include, but are not limited to: name, address, email and phone number; attorney name and contact information; as well as the an individual's account of the physical, emotional, and economic impacts of the crime with itemized losses, medical information, and supporting documentation, general location of individual's residence or work, personal and business impacts caused by the event, and suggested solutions to prevent or mitigate the damage; Tax Identification Numbers (individual social security number (SSN) or individual taxpayer identification number (ITIN)), adoption taxpayer identification number (ATIN), or employer identification number (EIN). More specific information and its uses can be found in the Information in the Information Technology table in Section 3.

Internal ENRD employees are the sole user-base who have administrative role-based access to Qualtrics. Based on management approval, DOJ contactors may be granted role-based, and limited, access to the data in Qualtrics as required by their involvement on ENRD teams. Employee data will only be accessed by ENRD's human resources and training teams. Simple polling data, appointment information, and design preferences will be accessed by ENRD survey creators. ENRD legal teams may have members from other agencies that will have access to the data through their participation on the ENRD team. ENRD litigation is referred by client agencies. Data collected in Qualtrics may be shared with the client agency as necessitated by their mutual agreement. Defendant tax information is securely transferred to an internal DOJ financial system for processing only. Solution statements and associated contact information will be collected and distributed to local community leaders by ENRD as noted in the survey's privacy statement.

ENRD conducted this Privacy Impact Assessment to document its use of Qualtrics, in accordance with Section 208 of the E-Government Act of 2002.

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.

ENRD's litigation mission includes civil and criminal enforcement investigations and actions, as well as defensive work on behalf of the United States government.[2] The information collected is used to accomplish activities inherent in the Division's investigations, litigation, and administrative support.

[2] ENRD's mission is to enforce the Nation's civil and criminal environmental laws, including the Clean Air Act, Clean Water Act, and hazardous waste laws. The mission also involves the protection of the Nation's natural resources and handling cases relating to tribal rights and resources. The Division's efforts result in significant public health and other direct benefits to the American people through the reduction of pollution across the Nation and the protection of important natural resources.

Collection, maintenance, and use of the information supports ENRD's litigation and administrative functions.

ENRD will use the Qualtrics service to collect and analyze data in employee engagement, retention, and other administrative functions. ENRD will conduct surveys on facets of workplace culture, work-life balance, and management. These examples include, but are not limited to training course performance, employee engagement, and diversity, equity, and inclusion, as well as appointment scheduling and simple polling for preferences on meeting times and locations or web interface or document designs. This data will guide management decisions to retain top talent, provide excellent workforce training, and improve administrative products and services.

For the public, ENRD will leverage the platform's security and flexibility to create customized solutions that will streamline ENRD's litigation support for both victims, defendants, and communities impacted by environmental crime while safeguarding their information. Examples of these public use cases include, but are not limited to:

- support litigation by collecting Victim Impact Statements on-line from potential victims of environmental crimes to present to the court;
- support enforcement by collecting a defendant's tax information from them and securely transmit it the IRS when a fine is levied against them; and
- support community-based problem solving by soliciting and collecting statements from members of an impacted community with identifying information for discussion and follow up with community leaders.

The general types of information collected, maintained, used, and/or disseminated through Qualtrics for the employee examples include: employee name; position; supervisory/non-supervisory; race, gender and age demographics; length of employment; choice of applicants; feedback on management and team performance, impressions of workplace and engagement; impacts diversity, equity, and inclusion initiatives have had. training course attended; preferences for meeting times and locations; day and time of select appointments; preference and feedback on design materials. Aggregate data may be shared within the Division to improve employee engagement, assess training efforts, and improve administrative services.

The general types of information collected, maintained used and/or disseminated via Qualtrics for litigation and sentencing purposes include: the victim's name, address, email, and phone number; the victim's attorney and contact information; as well as the victim's account of the details of the physical, emotional, and economic impacts of the crime with itemized losses, medical information, and supporting documentation. This data will be used to prosecute environmental crimes and provide statements for the impact the defendant's actions had on victims in determining sentencing. This directly supports ENRD's litigation mission of civil and criminal enforcement investigations and actions.

The general types of information collected, maintained used and/or disseminated via Qualtrics for defendant tax purposes include: names, addresses, phone numbers, email addresses, and Tax Identification Numbers (individual social security number (SSN) or individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN). In January 2021, the Tax Cuts and Jobs Act (TCJA) updated the Internal Revenue Code, so that taxpayers may not deduct amounts that, under court orders or settlement agreements, are paid to, or at the direction of, governments in relation to the violation of any law or the investigation or inquiry into the potential violation of any law. In addition, the final regulations also affect governments, governmental entities, and nongovernmental entities subject to the related reporting requirements. To

comply with this change, ENRD must report fine amounts levied against defendants to the IRS as a part of its litigation operations. To do this, ENRD must collect the defendant's information and transmit it to the IRS with the corresponding fine amounts, so the defendant receives a completed 1098-F form for their taxes. This information will not be stored beyond the amount of time required to transmit to IRS. It will not be shared with any other agency. This directly supports ENRD's litigation mission of criminal enforcement investigations and actions.

The general types of information collected for the Community Solution Statements include: name, email, phone number, general location of residence or work, how they were impacted by the event, and suggested solutions to prevent or mitigate the damage. This information supports the Administration's priority to protect overburdened and underserved communities from the harm caused by environmental crimes, pollution, and climate change. Sourcing solutions from the community for discussion by community leaders builds partnerships with community advocates and provides fair and equal treatment and involvement in the environmental decision-making process. Applying this technology to this mission allows data and solutions from community members who are intimately familiar with and affected by their communities' problems and challenges to be collected and counted in the decision-making process with local, tribal, state and Federal agencies. This directly supports the Department's Strategic Plan Objective 3.5: Advance Environmental Justice and Tackle the Climate Crisis by improving efforts to engage communities with environmental justice concerns and promote greater public participation in decisions affecting human health and the environment. Community Solution statements will be collected and distributed to local, tribal, state and Federal agencies by ENRD's staff.

While there are many ways to collect and analyze the types of data collected, using Qualtrics provides easier access for individuals to participate; secure data handling and storage of sensitive information; and streamlined data processing. Using the world wide web means that anyone with any type of internet connection -- home internet, cellular internet, or through a public library -- can participate in ENRD's litigation activities when needed. Additional methods of 'survey by text message' and scanning in paper forms to the digital service are also being developed, providing additional avenues of participation. Qualtrics support for providing surveys in multiple languages means individuals who are most at risk for being a victim of a crime have a way to participate in finding justice and resolution.

Previous methods of collecting this information required collecting paper surveys or having individuals email them to the legal team. Paper surveys are difficult to store and require a significant number of human hours to analyze. Emailed digital forms are easier to store, but email may not be a secure way to transmit sensitive data, especially Social Security Numbers. Qualtrics is a FedRAMP Moderate authorized, cloud-based digital survey service. Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with FISMA , OMB Circular A-130, and FedRAMP policy. Qualtrics is an optimal choice to collect and store sensitive information like personally identifiable, medical, financial, and employment information from the public. Qualtrics provides protections for the continued security of the data and privacy of employees and the public.

Qualtrics provide numerous tools for data processing and visualization to streamline the process converting data into actionable information. As a native digital tool, it provides real-time status information on the number of surveys collected and current results. Data visualizations can be applied to different types of questions to better understand the data and provide meaningful charts to decision-makers. A keyword search allows ENRD teams to find relative narrative responses. These tools can save thousands of hours of labor tallying the survey responses, identifying patterns, and creating cohesive narratives with intuitive dashboards and reports. This supports both ENRD's litigation and enforcement focus as well as its administrative functions.

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	28 U.S.C. §§ 51419; 42 U.S.C. § 7413(g); 5 U.S.C. § 552; 42 U.S.C. § 6973(d); 42 U.S.C. § 9622(d)(2); 42 U.S.C. § 9622(i).
Executive Order	12898 Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations (February 11, 1994)
Federal regulation	28 CFR, Subpart L; 28 CFR § 50.7; 28 C.F.R. § 16.41; 26 CFR, Part 1 Denial of Deduction for Certain Fines, Penalties, and Other Amounts; Related Information Reporting Requirements
Agreement, memorandum of understanding, or other documented arrangement	EPA-ENRD MOU, 42 Fed. Reg. 48942-44 (June 15, 1977)
Other (summarize and provide copy of relevant portion)	Justice Manual 512.620 (https://www.justice.gov/jm/justice-manual) Memorandum for Heads of Department Components Actions to Advance Environmental Justice (May 5, 2022) Memorandum for Heads of Department Components Comprehensive Environmental Justice Enforcement Strategy (May 5, 2022) DOJ Strategic Plan 2022-2026 https://www.justice.gov/doj/doj-strategic-plan/

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, C, and D	Employee satisfaction surveys may request this information. Victim Impact Statements will request the person's name.
Date of birth or age	X	A, C, and D	Employee satisfaction surveys may request this information. Victim Impact Statements may contain demographic information related to the victim's gender, race/ethnicity, and age, as well as other personal information.
Place of birth			
Gender	X	A, C, and D	Employee satisfaction surveys may request this information. Victim Impact Statements may contain demographic information related to the gender, race/ethnicity, and age, as well as other personal information.
Race, ethnicity, or citizenship	X	A, C, and D	Employee satisfaction surveys may request this information. Victim Impact Statements may contain demographic information related to the gender, race/ethnicity, and age, as well as other personal information.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	Social Security number is used to create tax documents for fines imposed as the result of litigation.
Tax Identification Number (TIN)	X	C	TIN is used to create tax documents for fines imposed as the result of litigation.
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C, and D	Victim Impact Statements will collect this information. This information is also collected from defendants to create tax documents resulting from the imposition of fines.
Personal e-mail address	X	C, and D	Victim Impact Statements will collect this information. This information is also collected from defendants to create tax documents resulting from the imposition of fines.
Personal phone number	X	C, and D	Victim Impact Statements will collect this information. This information is also collected from defendants to create tax documents resulting from the

			imposition of fines.
Medical records number	X	C, and D	Victim Impact Statements may contact health information or medical diagnoses related to injuries or conditions resulting from the crime.
Medical notes or other medical or health information	X	C, and D	Victim Impact Statements may contact health information or medical diagnoses related to injuries or conditions resulting from the crime.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	C, and D	Victim Impact Statements may contain employment/disciplinary information related to physical or emotional impacts of the crime.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C, and D	Victim Impact Statements may contain employment/disciplinary information related to physical or emotional impacts of the crime.
Certificates			
Legal documents	X	C, and D	Victim Impact Statements may contain additional legal documents and information related to the crime.
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	X	C, and D	Victim Impact Statements will collect this 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	Audit data would contain Admin user accounts used to create surveys and analyze survey responses to user ID.
- **User passwords/codes**	X	A	Audit data would contain Admin user accounts used to create surveys and analyze survey responses to user ID.
- **IP address**	X	A	Audit data would contain Admin user accounts used to create surveys and analyze survey responses to user ID.
- **Date/time of access**	X	A	Audit data would contain Admin user accounts used to create surveys and

			analyze survey responses to user ID.
- **Queries run**	X	A	Audit data would contain Admin user accounts used to create surveys and analyze survey responses to user ID.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Given of the varied nature of ENRD's work Qualtrics data could conceivably include almost any type of unclassified PII, and it is not possible to list with certainty every item of information that will be processed by the system.

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		Other DOJ Components		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):					

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	Internal ENRD employees are the sole user-base who have role-based access to data stored in Qualtrics. Defendant tax information is accessed only by required staff. Statements from individuals will be managed by members of ENRD legal teams.
DOJ Components	X			Statements may be exported and collated with representatives from other components on the legal team. Defendant tax information is transferred to an internal DOJ financial system for processing.
Federal entities	X			Statements may be exported and shared other agencies that referred the case to ENRD for prosecution or are involved with the project. Defendant tax information is securely transferred to an internal DOJ financial system for processing and then to the Internal Revenue Service.
State, local, tribal gov't entities	X			Statements may be exported and shared with client agencies that referred the case to ENRD for prosecution and in some instances other state, local and tribal entities in the locality of the environmental event.
Public	X			Solutions statements collected form the public will be shared with the public, as indicated in the privacy statement at the beginning of the survey.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			The Victim Impact Statements will be exported and collated for use in litigation.
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.

No information collected will be released 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.

A Privacy Act § 552a(e)(3) notice for individuals will be included at the start of every form explaining what data will be collected and the purposes it will be used for. Community Solution Statement forms will also emphasize that responses collected through the form are not confidential and will be shared with local agencies. If a survey is offered in a language other than English, this notice will be translated into the target language of the survey for use with that translation of the survey.

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.

Only the defendant tax form information is compulsory for defendants. Victim Impact and Community Solution Statements are voluntary for participants. Victim Impact Statements are only used in the litigation and sentencing of an environmental crime. The victim can make a choice to not fill out the form if they do not want their information used for this purpose. They may opt out of the form after reading the privacy statement or not submit their responses after reviewing the questions and information requested. Community Solution Statements responses are community-generated solutions to environmental events. The agencies involved with these will protect PII, but the submissions themselves are not confidential and will be shared with local government, state government, and references in court filings. Respondents are not required to answer all questions and may submit additional information or recommendations in their response. They may opt out of the form after reading the privacy statement or not submit their responses after reviewing the questions and information requested.

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.

Individuals can gain access to their information or request correction by contacting ENRD's Law & Policy Section which handles FOIA and Privacy Act requests. Instructions for FOIA requests can be found on ENRD's FOIA page: https://www.justice.gov/enrd/enrd-foia . Individual requests to update data can be made by authorized ENRD staff in the Qualtrics

platform as outlined in the individual's request.

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):** A FedRAMP ATO qualifies cloud service providers (CSPs) to work with any federal agency. Agencies can review and reuse CSO security packages once they are designated as "Authorized" within the FedRAMP Marketplace by issuing their own authorization to use the product. FedRAMP Authorized: 06/29/2018 **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:**
X	**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:** Yes, this system is not subject to an individual ATO. It is a cloud-based service provided by a vendor. The initiating agency provided an ATO to FedRAMP Yes, NIST privacy controls have been implemented and assessed. This service is authorized at the Moderate level by FedRAMP. FedRAMP is a government-wide program that standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with FISMA and OMB Circular A-130. A third-party, independent assessor documents the service's compliance with the FIPS 199 categorization and security controls as a part of the authorization.
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 Qualtrics digital service is authorized at the Moderate level by FedRAMP. Vendors and the FedRAMP PMO use the FIPS 199 categorization to ensure their services meet the minimum security requirements for the data processed, stored and transmitted on them. A third-party, independent assessor documents the service's compliance with the FIPS 199 categorization and security controls.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** To maintain compliance with FedRAMP, CSPs must monitor their cloud system's security controls, assess them on a regular basis, and demonstrate the security posture of their service

	offering is continuously acceptable. CSPs satisfy this requirement by implementing Continuous Monitoring (ConMon) activities, as documented in FedRAMP's ConMon requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf) and the cloud system's ConMon plan.
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:** To maintain compliance with FedRAMP, CSPs must monitor their cloud system's security controls, assess them on a regular basis, and demonstrate the security posture of their service offering is continuously acceptable. CSPs must review and update auditable events annually or whenever there is a change in the threat environment. Changes to the auditable event list must be recorded in the System Security Plan. CSPs must record the date that the auditable event review meeting takes place in the System Security Plan. Meeting notes with information about who attended the meeting must be archived. CSPs must have a third-party assessor organization assess a subset of their security controls annually. More information is available in the FedRAMP Continuous Monitoring Strategy Guide.
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 privacy training specific to this 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?

As a FedRAMP Authorized CSP, Qualtrics has implemented security and access control standards as outlined by NIST. These include physical access controls, monthly visitor access review, audit logs, 60-day changing of passwords, the disablement of accounts inactive over 90 days, vulnerability scans, and penetration testing, and uses https to ensure that data is encrypted in transit and at rest. These are outlined in the Continuous Monitoring Strategy Guide.

ENRD will use role-based user management to ensure only necessary staff have access to this specialized data.

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.)

Qualtrics functions as a "pass-through system." Its sole function is to receive and integrate data and export the resultant product to yet another independent system. GRS 5.2, item 020 covers such a system's content.

The defendant tax information is a non-record and will be on a 30-day schedule to ensure the information is successfully transferred to the terminal system. Once confirmed, the data will be deleted form the Qualtrics platform.

Victim Impact Statements are managed as part of a criminal case and are part of Permanent schedule. The legal team will export the data from Qualtrics to submit to the court. The resulting document will be included in case documents as part of the document management system referenced by DJ number. N1-60-88-1 Item No. 198 Justice Records Control Schedule Class 198 Criminal Environmental Matters.

Community Solution statements will be part of a project. The data will be exported form Qualtrics and then be managed as part of the project record retention. This record schedule is currently being developed by the Department.

Employee surveys and feedback are a record and managed under the General Records Schedule Section 2.2 and 2.6.

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:

Employee engagement, training effectiveness, and diversity, equity and inclusion data was previously collected with prior survey software under ENRD's existing SORN.

This Victim Impact Statements data was previously covered the existing SORN for ENRD. This data was collected via documents completed by witnesses and emailed or postal mailed to the Division's legal teams.

DOJ/ENRD-003, *Environment & Natural Resources Division Case & Related Files System*, last published in full at 69 Fed. Reg. 26179 (May 11, 2004).

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?

a. Potential Threats Related to Information Collection

The privacy risks associated with information collected within Qualtrics primarily relate to the loss of confidentiality, integrity, and availability of data. Access by unauthorized entities to sensitive data, including personal information collected for investigation or litigation potentially could lead to destruction of that data, compromised identities, exposure of sensitive court records and personal data, and/or disruption to an ongoing litigation. ENRD choose Qualtrics to collect and store this data because it is a FedRAMP Moderate authorized, cloud-based digital survey service. For FedRAMP Moderate authorized systems, FIPS 140-validated encryption is required for federal data at-rest [SC-28], data in-transit [SC-8(1)], and authentication [IA-2(11)] as required Security Control-13. FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with FISMA, OMB Circular A-130, and FedRAMP policy. Using this service provides a significantly higher level of protection than using other commonly available tools to collect this essential data.

Access to SSNs is restricted and only available to certain users with a need to know, for administrative purposes. SSNs are not viewable outside of users who are permitted access in order to perform key administrative functions. SSNs stored in ENRD applications are encrypted, and the Division continues to seek alternative methods to avoid the use of SSNs.

b. Potential Threats Related to Use of the Information

All applications of the Qualtrics platform will have a specific purpose to limit their data collection. Data is securely housed in its secure, cloud storage for processing, analysis, and export by authorized ENRD staff. ENRD provides privacy notices through system of records notices (SORNS), published on DOJ's system of records website (https://www.justice.gov/opcl/doj-systems-records), and PIAs. Additionally, personnel are required to take Computer Security and Awareness Training (CSAT), which incorporates privacy. All surveys will have a privacy notice at the start of the form stating what data is being collected, how it will be used, and who it will be shared with. The ENRD's use of Qualtrics to collect only the data that is required to complete the tasks at hand. When an ENRD employee departs from the Division, appropriate measures are taken to deactivate the user access and accounts to ENRD information.

c. Potential Threats Related to Dissemination

ENRD establishes control over information contained in Qualtrics by strictly managing access controls, limiting permissions to only surveys that a user requires, and ensuring compliance with DOJ two-factor identification and authentication requirements. Further, privacy specific analysis and reporting is maintained within an authorized Cybersecurity Assessment and Management (CSAM) profile. The capability to generate reports from Qualtrics is controlled by permission and limited to authorized personnel.