U.S. Department of Justice

Privacy Impact Assessment
for the
Defined Monetary Assistance Victims Reserve

Issued by:

Michelle Ramsden
Senior Counsel, Office of Privacy and Civil Liberties

Approved by: Michelle Ramsden
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 27, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how it operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Under Federal law, victims of child pornography offenses are entitled to full and timely restitution from defendants charged and convicted in Federal court, including restitution for losses caused by conduct such as the possession, receipt, viewing, transportation, and distribution of these images.[1] Restitution is imposed upon an individual criminal defendant by a Federal court at the time of sentencing, and the obligation to pay restitution is part of the defendant's criminal sentence.[2] The Federal Government bears the burden of proving that the defendant owes restitution to a victim, although a defendant can agree to pay restitution as part of a plea agreement.

The Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018 ("AVAA") created an alternative system to allow victims of trafficking in child pornography to obtain some measure of compensation (called ''defined monetary assistance'' or "DMA") without having to prove their losses. For this purpose, the AVAA established the Defined Monetary Assistance Victims Reserve ("Reserve") to provide defined monetary assistance to eligible individuals who are depicted in child pornography that is the basis for certain convictions under 18 U.S.C. chapter 110. Under the terms of the statute, victims of these types of child pornography offenses can choose whether to present their full restitution claims in court through prosecutors or to obtain a one-time payment of defined monetary assistance. The determination regarding victim eligibility for the DMA payment is made by the court. The Act provides that the ''Attorney General shall administer'' this Reserve;[3] therefore, the Department will provide payment from the Reserve to a victim pursuant to a court order issued and upon receipt of the requisite information from the claimant.

Pursuant to the Department's instructions, claimants may choose to request that the Department present a motion outlining the basis of a claim to a court for the court's determination of eligibility. The Department will review the request and may follow up as needed to seek additional information directly from the claimant or the claimant's authorized representative in order to resolve any gaps in the claimant's supporting information. A claim is complete where it is supported by all information required by the claim form and by responses to follow-up requests for information. After the Department has exhausted reasonable efforts to obtain any needed additional information from the claimant, the Department will use reasonable efforts to identify a federal child pornography trafficking case in which an image of the claimant appears. The Department will consider any case(s) identified by the claimant as well as any in which the Department has independent information linking the claimant to a federal child pornography trafficking case. If, based on the information in the request, the claimant might be eligible for defined monetary assistance as a result of more than one case, the Department, in its sole discretion, will decide in which case it will present the claim.

---

[1] See 18 U.S.C. 2259.
[2] See id.; see also 18 U.S.C. 3663A.
[3] See 18 U.S.C. 2259B(c).

Once the Department identifies an appropriate case, the Department will present the claimant's claim, by way of motion and attachments filed under seal, to the district court, which may then issue an order affirming the claimant's eligibility for payment. In the event that a motion is denied by the district court, the Department may decide to appeal a ruling by a district court denying the claimant's eligibility for defined monetary assistance. The Department will make reasonable efforts to consult with the claimant (and the claimant's authorized representative, if applicable), on the issue of appeal. Depending on the basis for the court's ruling, the Department may seek to present the claim underlying a denied motion in another case when it would be appropriate to do so. The Department will also make reasonable efforts to consult with the claimant or authorized representative about any decision to present a claim in another case. If the court issues an order of payment, the Department will pay the victim the defined monetary assistance from the Reserve, as specified in the order. Payment will typically be made via electronic funds transfer facilitated by the Department of the Treasury, but the Department may use other methods (e.g., physical check) depending on the circumstances.

A Privacy Impact Assessment is being conducted pursuant to the e-Government Act of 2002 because this project involves the Department's collection, maintenance, use, and dissemination of information, in identifiable form, pertaining to members of the public using information technology.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or 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.

There will be two methods to collect information from claimants who apply for defined monetary assistance; both methods will collect the same information. One method uses a paper claim form, submitted by mail, and the other uses an online portal; however, in both cases, the claim will be processed by the Department within the online portal. The online portal's architecture is centered on Microsoft's Dynamics 365 Customer Service Software as a Service (SaaS) cloud offering hosted in Microsoft's Government Community Cloud (GCC) for high impact systems and is supplemented with Microsoft Azure Government cloud services as required.

Types of information requested of the claimant include the following: names, addresses, dates of birth, dates of death, social security or tax identification numbers, bank account information, and related supporting documents to prove eligibility and effectuate payment. Claimants who choose to use the online portal will be authenticated using OJP's secure Digital Identity and Access Management Directory (DIAMD).[4] Claimants will then have the option, in the external interface of the portal, to complete, save progress, submit, and update their claim form; submit supporting documents, including information required for payment; receive reminder emails prompting further action or notifying claimants of progress on their claim; view the status of their claim; and receive guidance on use of the portal.

[4] DIAMD is covered by separate privacy compliance documentation.

Upon submission in the online portal, a claim and its supporting documents are reviewed in the internal interface of the portal by a claims manager at the Executive Office for U.S. Attorneys (EOUSA). Upon receiving paper-based claims, claims managers scan and upload the information contained within the paper claim form into the electronic system supporting the online portal on behalf of the claimant or authorized representative. The claims manager reviews the documents and either requests further information from the applicant, recommends referral to a U.S. Attorney's office (USAO), or rejects the claim. Referred claims are transmitted directly to the designated Assistant U.S. Attorney (AUSA) through the online portal.

Upon receipt of the claim and supporting documents, the designated AUSA reviews the information in the online portal. If the claim and supporting documents are incomplete or cannot be matched with a qualifying case, the AUSA either returns the claim to EOUSA or requests more information from the claimant. If appropriate, the AUSA prepares a pleading for the district court's consideration regarding whether the claimant is qualified to receive DMA. The district court considers the pleading and issues its order, either finding the claimant is eligible to receive DMA, or denying eligibility. Upon the issuance of the court's order, the designated AUSA transmits the court's order, claim for DMA, and supporting documents back to a secondary reviewer within EOUSA Legal Programs through the online portal.

If the court finds the claimant eligible and orders the payment of DMA, the claimant is required to submit a completed Automated Clearing House (ACH) banking form to the secondary reviewer, who then transmits that information to the Office for Victims of Crime using the online portal to effectuate payment. If the court denies the order, the reviewer determines if another USAO should process the claim and supporting documents for judicial consideration.

Regardless of the outcome of the claim, the claimant or authorized representative is notified at equivalent intervals either using the online portal or, if the claim form was submitted by mail, using the method most appropriate and accessible to the claimant or authorized representative (either the online portal, the telephone, or First-Class, Certified, or Registered Mail).

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	The Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. 115-299.
Executive Order	
Federal regulation	At the time of this PIA, Final Rule in progress.
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	C, D	Victims', victim's representatives', and claimants' names
Date of birth or age	X	C, D	Victims' dates of birth
Place of birth	X	C, D	Victims' places of birth
Gender	X	C, D	Victims' gender, as assigned at birth
Race, ethnicity, or citizenship	X	C, D	Victims' citizenship
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	Victims' and claimants' SSNs
Tax Identification Number (TIN)			
Driver's license	X	C, D	Victims', victim's representatives', and claimants' driver's license numbers
Alien registration number	X	C, D	Victims', victim's representatives', and claimants' alien registration numbers
Passport number	X	C, D	Victims', victim's representatives', and claimants' passport numbers
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C, D	Victims' and claimants' personal mailing addresses
Personal email address	X	C, D	Victims' and claimants' personal email addresses
Personal phone number	X	C, D	Victims' and claimants' personal phone numbers
Medical records number			
Medical notes or other medical or health 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
Financial account information	X	C, D	Victims' and claimants' bank account information
Applicant information			
Education records			
Military status or other information	X	C, D	Victims' and claimants' employment and/or military status may be apparent in information collections
Employment status, history, or similar information	X	C, D	Victim's representatives' employment status may be apparent in information collections
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents	X	C, D	Legal documents related to the case(s) identified by the claimant, and other cases identified by the Department
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	Defendants' criminal history information may be collected as supporting documentation
Juvenile criminal records information	X	C, D	Defendants' criminal history information may be collected as supporting documentation
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information	X	C, D	Information relating to criminal investigations or prosecutions may be collected as supporting documentation
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	Information relating to criminal investigations or prosecutions may be collected as supporting documentation
Procurement/contracting records			
Proprietary or business 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
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, C, D	User ID of claimants or claimant representatives will be visible to individual claimants/claimant representatives, and those government employees and contractors with access to the online portal.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A, C, D	Date, time, and access of individual claimants or claimant representatives will be visible only to individual claimants or claimant representatives and to those government employees and contractors with access to the online portal.
- **Queries run**	X	A	
- **Contents of files**	X	A, C, D	Claimants or claimant representatives will have visibility only into the contents of those files they submit. Contents of files will be visible to those government employees and contractors with access to the online portal.
Other (please list the type of info and describe as completely as possible):	X	C, D	Claimants will be assigned unique case numbers, which will be used to track and transmit their claims

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	X	Online	X
Phone		Email			
Other (specify): As described above, information will be collected directly from individuals through the mail or an online portal.					

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): As described above, information related to the case(s) identified by the claimant, and other cases identified by the Department may be implicated.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): As described above, information may be collected from claimants or victims' representatives who are not the subject of the information.					

Section 4: Information Sharing

4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			Information may be shared with other component personnel on a case-by-case basis only to the extent required to facilitate processing and payment of a claim. This sharing will occur through the designated online portal.
DOJ Components	X			Information may be shared with other DOJ personnel on a case-by-case basis only to the extent required to facilitate processing and payment of a claim. This sharing will occur through the designated online portal.
Federal entities				
State, local, tribal gov't entities				
Public	X			Information about a claim may be shared with the relevant victim, claimant, or claimant's representative only to the extent required to facilitate processing and payment of a claim. This sharing will occur through the designated online portal.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Information about a claim may be shared with the relevant claimant's representative only to the extent required to facilitate processing and payment of a claim. This sharing will occur through the designated online portal.

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.**
				Information about a claim may also be shared with judicial tribunals via sealed pleadings only to the extent required to facilitate a tribunal's decision on the eligibility of a claimant.
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 from the Reserve 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.

The paper-based and online forms used to collect information pertaining to the Reserve will include specific notice to individuals about the collection, use, sharing or other processing of their PII in the form of a Privacy Act (e)(3) notice, approved by the Office of Privacy and Civil Liberties.

Further, the Department of Justice's website includes a website privacy policy which, at the time of this PIA, is available at:

https://www.justice.gov/doj/privacy-policy.

General notice will be provided to the public about the collection, use, sharing or other processing of their PII in the form of a Federal Register System of Records Notice (SORN), entitled JUSTICE/USA-020 – Child Pornography Victims' Reserve Records, which, at the time of this PIA, is in pre-publication review. That SORN will be published on the Department

of Justice's Systems of Records webpage at:

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

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.

All claims will be processed at the request of a claimant or claimant's representative on the basis of consent. The information requested in the online forms is the minimum information necessary to facilitate the processing and payment of claims through the Reserve. Without this PII, the Department will be unable to accurately identify the relevant victim and case(s) and will be unable to complete its processing of the claim.

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.

The process of providing a claimant with access to information held by the government will be subject to all applicable laws and regulations, including the Privacy Act of 1974, 5 U.S.C. 552a, and subpart B of part 16 of title 28, Code of Federal Regulations.

Pursuant to the relevant System of Records Notice, individuals may seek access, correction, or amendment of records related to the Reserve that pertain to them by submitting a request in writing, by regular mail addressed to the FOIA Public Liaison, FOIA/Privacy Staff, Executive Office for United States Attorneys, U.S. Department of Justice, 175 N St. NE, Suite 5.400, Washington, DC, 20530 or online at https://eousafoia.usdoj.gov/. Procedures for making a written request are located on EOUSA's website: https://www.justice.gov/usao/resources/making-foia-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.

The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):

The Reserve is in the process of obtaining an ATO.

If an ATO has not been completed, but is underway, provide status or expected completion date:

An ATO is anticipated on July 31, 2024.

Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:

The Reserve has one outstanding POAM to facilitate compliance with DOJ security requirements around audit logging and continuous monitoring. This POAM will track the system's integration with Splunk and ensure compliance with audit log ingestion and alert monitoring requirements.

This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:

N/A

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 actual elements of information within the Reserve have been assigned a FIPS security categorization of moderate, pursuant to the "high water mark" standard. This categorization is based on universal categorization of Moderate assessments in Confidentiality, Integrity, and Availability for both its Personal Identity and Authentication as well as its Official Information Dissemination Information Types.

However, recognizing the innate sensitivity of any information associated with victims of child pornography, the Reserve will be stored in the Government Community Cloud (GCC)-High environment, which is designed to handle data up to the Department of Defense (DOD) Impact Level 5 and imparts significant security beyond what is required for a moderate baseline.[5]

Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:

The Reserve is subject to an annual internal assessment of OJP's defined Core Controls conducted throughout the course of the Fiscal Year. DOJ's annual Core Control assessment includes the testing and evaluation of the security and privacy controls safeguarding the information within the system. In addition, OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting DMAVR in accordance with FedRAMP Continuous Monitoring requirements.

Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:

The Reserve enables auditing of actions taken by an individual, including unauthorized modifications to claimants' information. The audit trail captures any changes to the victims'

[5] DOD IL5 designates higher sensitivity controlled unclassified information, mission-critical information, and national security systems.

data by DOJ personnel. Upon the above-mentioned integration with Splunk, OJP Cybersecurity teams will monitor logs in accordance with DOJ security control requirements, which require monitoring on a weekly basis. The Reserve also provides reporting of duplicate or incomplete applications and aging case reports to prevent the unnecessary retention of superfluous or outdated information in the system.
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. All DOJ contracts that implicate PII, including contracts by which the Department obtains embedded contract personnel who process the victim PII implicated by the Reserve, are required under DOJ Acquisition Procurement Notice APN-21-07A to include the DOJ-02 Contractor Privacy Requirements clause, which satisfies the relevant requirements of the Privacy Act and other applicable law, regulation, and policy.
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: All Department personnel whose primary job responsibilities affect crime victims and witnesses, or who in the course of their duties are expected to come into contact with victims and witnesses, must complete training on the Attorney General Guidelines for Victim and Witness Assistance, which provide relevant and valuable guidance on handling victim information.

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?

Although the actual elements of information within the Reserve have been assessed at a FIPS security categorization of moderate, the Department recognizes the innate sensitivity of any information associated with victims of child pornography. Therefore, the Reserve will be stored in a high security environment designed for, and secure enough to handle information up to the DOD Impact Level 5.

Further, claimant submissions will not be made public and will be protected and used only on a "need-to-know," as needed basis in accordance with applicable law, including the Privacy Act of 1974, 5 U.S.C. 552a. Pursuant to 5 U.S.C. 552a, 18 U.S.C. 3509(d)(1), and 18 U.S.C. 3771(a)(8), the Department will not disclose to the public the names of the individuals who have requested DMA from the Reserve or the names of the decedents for whom defined monetary assistance is sought from the Reserve, except as necessary to process a request or claim or obtain a court order, to bring a criminal or civil case against an individual for

obtaining defined monetary assistance by fraud, or pursuant to law or court order.[6]

Upon receipt, paper claims and supporting documents will be scanned by EOUSA, uploaded to the online portal, and transmitted to the qualifying district for the AUSA's review; thereafter, the paper documents will be destroyed using a secured shredding process as soon as is feasible pursuant to the relevant records retention schedules.

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

The records retention schedule covering records related to the Reserve is currently under development. Until a records retention schedule is approved by the National Archives and Records Administration, records related to the Reserve will be retained for the purpose of processing new claims that may be related to existing records. Once the records retention schedule is complete, records will be destroyed according to the schedule.

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.

A unique case number will be assigned to each claim received by the Reserve. This case number will be used to track and retrieve information relevant to the claim.

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:

The JUSTICE/USA-020 – Child Pornography Victims Reserve Records SORN has been submitted for publication and will be complete prior to operation of the system.

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

[6] For example, the fact that a victim has received defined monetary assistance must be introduced in a federal criminal proceeding where the amount of the victim's losses is at issue.

being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Privacy Risk: Overcollection of information.

Mitigation: Overcollection of information is a risk wherever members of the public enter information directly into a form, or mail or email information to the Department. In order to limit the risk of overcollection of information, the online portal will solicit from a claimant only the information required to process a claim. To mitigate the risk of claimants providing superfluous information, the online form has been drafted with character limitations and minimal free-text fields.

Privacy Risk: Receipt of unencrypted Social Security Numbers (SSNs).

Mitigation: The Reserve enables claimants to submit applications for, and, if eligible, receive DMA. In order to distribute DMA to eligible claimants, Tax Identification Numbers (TINs) or SSNs are required; because some claimants and authorized representatives do not have a TIN that is different from their SSN, SSNs are sometimes collected to facilitate payment.

Upon receipt of claims submitted by mail or email, the Department will restrict access to SSNs to DOJ claim processors with a need-to-know the information related to each individual claim. All information in the system, including SSNs, is encrypted at rest; and where required, the Department will transmit SSNs exclusively by encrypted email.

Privacy Risk: Unauthorized access, misuse by authorized user, or compromise of data.

Mitigation: Access to information collected by the Reserve is restricted to only those employees, as designated in Section 4, with a need to know the information to process the claim and is further restricted by role and tasks necessary to carry out an employee's duties (e.g., SSNs are available only to designated claim processors). As described above, paper claims and supporting documents will be scanned, uploaded to the online portal, and transmitted through the portal to enable processing of the claim; thereafter, any physical copies will be destroyed using a secured shredding process. AUSA recipients of claim information will store all information on a secured drive or, if they must print any of the materials received, in a locked file cabinet until they are destroyed.

In addition to annually required DOJ-wide cybersecurity awareness training, regular privacy training is provided to all employees and contractors to remind them of their obligations to protect data and minimize the use of PII wherever possible. These steps also mitigate the risk of either purposeful or

inadvertent compromise of data. In addition, the Department maintains a robust breach response process to mitigate any potential harm to individuals as a result of an actual or suspected breach.