United States Department of Justice

U.S. Parole Commission

Privacy Impact Assessment
for the
Offender Management System (OMS)

Issued by:
Helen Krapels,
General Counsel,
Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 16, 2022

Section 1: Executive Summary

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

The Offender Management System (OMS) allows the U.S. Parole Commission (USPC or "Parole Commission" or "Commission") to process and store electronic information on offenders (convicted of violating Federal and District of Columbia (DC) laws), witnesses, and victims. OMS is a role-based case management system. Information collected on such individuals include the following: unique identifying numbers for offenders, personal data, work-related data for offenders, contact information for victims and witnesses, and other information on offenders including prior arrest records, drug test results, and any other records on conduct, treatment, and work history while incarcerated or on supervision. This support involves processing transactions necessary to obtain an offender's release, and their subsequent supervision after release. The mission of the USPC is to promote public safety and strive for justice and fairness in the exercise of its authority to release and supervise offenders under its jurisdiction.

USPC conducted this Privacy Impact Assessment to assess and mitigate the risks to the personally identifiable information (PII) collected in this system, which includes but is not limited to the information described above along with, individual names, specific descriptions of criminal allegations against individuals, and, in limited circumstances, other individual identifiers, such as dates of birth (DOBs), and contact information.

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.

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

The U.S. Parole Commission is required by law (18 U.S.C. § 4207) to consider all relevant and available information on an offender in order to make informed decisions on release and supervision of the offender. Possessing complete and accurate information is essential for the Commission to evaluate each individual case and determine appropriate action. The OMS gives the Parole Commission the ability to process and store electronic information on offenders, witnesses, and victims pertaining to U.S. Code and District of Columbia Code sentenced prisoners and releasees.

Information is collected on such individuals for the following reasons:

(1) make parole release determinations and decisions on release conditions; (2) make decisions on revoking parole and granting early termination of parole; (3) make decisions on revoking supervised release for D.C. offenders and setting new prison terms and new terms of supervised release for such offenders; (4) automate information sharing with U.S. Marshals Service to facilitate execution of warrants; (5) perform data analysis on location of crimes; (6) perform data analysis to determine effective treatment options; (7) share analytical information and data with other agencies; (8) speed up internal processing of records, decisions, and Freedom of Information Act (FOIA) requests; (9) track recidivism rates; and (10) provide more accurate victim information so that victims can be notified of hearings and decisions. Additional details regarding the types of information collected on these individuals are described in the table in Section 3.

The USPC OMS is populated from the following data sources: the District of Columbia's Criminal Justice Coordinating Council (CJCC) and Court Services and Offender Supervision Agency (CSOSA),[1] the Federal Bureau of Prisons (BOP),[2] and direct input by USPC staff, including digitizing paper files originally created by USPC staff. Data is organized by USPC staff within logical folders sorted by the inmate registration number and name. The USPC staff is responsible for maintaining and updating the logical folders as needed.[3] Cybersecurity and privacy controls on information access and data management are specified within memorandums of understanding and non-disclosure agreements for individuals (including USPC staff) and Federal, state, and local agencies requiring or requesting information from OMS.

OMS is a case management system internal to USPC, accessible only by Parole Commission staff. It is not a public facing system or does it provide website for the public to access. Federal, state, and local

---

[1] Court Services and Offender Supervision Agency (CSOSA) for the District of Columbia Exchange: OMS receives CSOSA Alleged Violation Reports (AVR) from Criminal Justice Coordinating Council (CJCC) via a web services link. Devices on each are authenticated via exchange of public certificates. CSOSA is an independent Executive Branch agency responsible for supervising DC parolees (accounts for 70% of all USPC case load). CSOSA assumed the adult probation function from the D.C. Superior Court and the parole supervision function from the D.C. Board of Parole (which has been dissolved).
CJCC plays an important role in facilitating an independent collaborative forum for stakeholders to address the District's longstanding and emerging public safety issues. In 2001, the DC Council established the CJCC as an independent agency with the Mayor as the chair and certain government agencies as its members. The CJCC is primarily a forum for the District's various criminal justice agencies to identify and address public safety issues that involved multiple criminal justice agencies. It acts as somewhat of a clearing house and data repository for various DC criminal justice agencies.
[2] Bureau of Prisons (BOP) Sentry System: OMS operators will manually download the Parole Hearing Docket on a weekly basis from the BOP. The file is then uploaded to OMS database and the offender records will be populated automatically. The USPC system administrator has been assigned a user account for the BOP mainframe. This is strictly one-way communications (receive only) from BOP.
[3] USPC staff includes properly vetted contractors and USPC federal employees.

agencies (hereinafter "requestor") submit requests to USPC. USPC staff then access OMS to retrieve the needed data to send back to the requestor.

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
X	Statute	18 U.S.C. § 4203(e)(1); §§ 4204(b)(5), (6); § 4205(e); § 4206(a), (c); § 4207; § 4209(a); § 4211(c).
	Executive Order	
X	Federal Regulation	28 C.F.R. § 2.19
X	Agreement, memorandum of understanding, or other documented arrangement	Interconnect agreements with Criminal Justice Coordinating Council (CJCC) and Court Services and Offender Supervision Agency (CSOSA) that specify the acceptable use, collection, and storage of all data.
	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	Name
Date of birth or age	X	C&D	Date of birth, age
Place of birth	X	C&D	Place of birth
Gender	X	C&D	Gender
Race, ethnicity, or citizenship	X	C&D	Race, ethnicity citizenship

(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
Religion		C&D	Religion
Social Security Number (full, last 4 digits or otherwise truncated)	X	C&D	Social Security Number (full, last 4 digits)
Tax Identification Number (TIN)			
Driver's license	X	C&D	Driver's license
Alien registration number	X	C&D	Alien registration number
Passport number	X	C&D	Passport number
Mother's maiden name	X	C&D	Mother's maiden name
Vehicle identifiers			
Personal mailing address	X	C&D	Personal mailing address
Personal e-mail address	X	C&D	Personal e-mail address
Personal phone number	X	C&D	Personal phone number
Medical records number	X	C&D	Medical records number
Medical notes or other medical or health information	X	C&D	Medical notes, other medical health information
Financial account information	X	C&D	Financial account information
Applicant information			
Education records	X	C&D	Education records
Military status or other information	X	C&D	Military status
Employment status, history, or similar information	X	C&D	Employment status, and history
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	C&D	Mobile device identifiers,
Web uniform resource locator(s)			Web uniform resource locator(s)
Foreign activities	X	C&D	Foreign activities

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C&D	Criminal history, arrests, criminal charges, treatment information, Parole or supervised release supervision information, File or case ID, federal prison identification
Juvenile criminal records information	X	C&D	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&D	witness statements, witness contact information, treatment information, parole, or supervised release supervision information
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C&D	Photographs
- **Video containing biometric data**	X	C&D	Police surveillance video
- **Fingerprints**	X	C&D	Fingerprints
- **Palm prints**	X	C&D	Palm prints
- **Iris image**			
- **Dental profile**			

(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
- **Voice recording/signatures**	X	C&D	Voice recording, signatures
- **Scars, marks, tattoos**	X	C&D	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	User ID[4]
- **User passwords/codes**			
- **IP address**	X	A	IP address
- **Date/time of access**	X	A	Date/time of access
- **Queries run**	X	A	Queries run
- **Content of files accessed/reviewed**	X	A	Content of files accessed/reviewed
- **Contents of files**	X	A	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	X	Hard copy: mail/fax	X	Online	
Phone	X	Email	X		
Other (specify): X OMS receives CSOSA Alleged Violation Reports (AVR) from Criminal Justice Coordinating Council (CJCC) via a web services exchange.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	

[4] USPC uses Personal Identity Verification (PIV) cards consistent with Homeland Security Presidential Directive-12 (HSPD-12) to allow access into OMS. The system collects user sign on information, but does not retain that information in its system boundary.

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

Non-government sources:					
Members of the public	X	Public media, Internet	X	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	USPC Staff access the information via individual login accounts supported by Personal Identification Verification (PIV) card or single sign on methodology to assist the USPC in making decisions.

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.**
DOJ Components	X			The Commission's decisions are communicated by email to other DOJ components to assist in the performance of their duties as a result of the Commission's decision. When a decision is issued, recipients[5] are selected and the decision is automatically sent to them. OMS data is shared case-by-case basis with ATF, FBI, BOP, and other components in DOJ as needed.
Federal entities	X			The Commission's decisions are communicated by email to other DOJ components to assist in the performance of their duties as a result of the Commission's decision. When a decision is issued, recipients are selected, the decision is then automatically sent to them.
State, local, tribal gov't entities	X	X		Information is communicated by mail, fax, or email per request by non-federal criminal justice agencies. OMS data (offender violation information) is sent to CJCC when CJCC requests the data in bulk via secure VPN. CJCC may then transmit back that data file to OMS after updating offender information. This two-way, transactional sharing of files continue as needed.[6]

[5] For this table, "recipients" do not include offenders, although offenders may receive the information from the initial recipient. Recipients in DOJ components and other federal entities are federal employees who will use the information for a criminal justice purpose.

[6] Approved CJCC and OMS analysts handling an offender's case file may edit the case file as needed. Within a case file there could be the following documents: Allegations of Violation Report (AVR), Notice of Action (NOA) Pre-Sentence Investigation (PSI) report, the Judgment and Commitment Order (J&C), and Notices of Action (NOA) are all types of requests sent between CJCC and OMS. Information is transmitted encrypted over Secure Sockets Layer (SSL).

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.**
Public	X			Information is communicated by mail or email per a request from the public (FOIA and first party requests).
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Information is communicated by email or mail. OMS data is shared case-by-case basis as needed such as in a lawsuit where USPC provides exhibits of documents stored in OMS. USPC also provides documentation to prisoners or their attorneys prior to their hearings to comply with disclosure laws and regulations.
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.

This information will not be released to the public for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

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

Generalized notice is provided pursuant to various USPC system of record notices published in the Federal Register. Notice has also been given that docket sheets, hearing schedules maintained in OMS

are covered by JUSTICE/PRC-001, "Docket, Scheduling and Control," 52 Fed. Reg. 47182, 281 (12-11-1987), 66 Fed. Reg. 8425 (1-31-2001), 72 Fed. Reg. 3410 (1-25-2007) (rescinded by 82 Fed. Reg. 24147), 82 Fed. Reg. 24147 (5-25-2017). A full list of USPC SORNs are available here: https://www.justice.gov/opcl/doj-systems-records#PRC.

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.

Offenders do not have the opportunity to decline the collection of information due to the nature of the proceedings.

Victims can request any statements provided by them to be confidential, and the Parole Commission will protect the identities and locations of victims. Victims can also decline the request to provide statements to the Parole Commission. However, anything provided to the Parole Commission may be disclosed to the prisoner/parolee because they have a statutory and due process right to know what information the Parole Commission has considered for its decisions.

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 who are being considered for some sort of action by the USPC ordinarily will have a hearing at which they can dispute the accuracy of the information maintained by the USPC per 28 CFR §2.19(c). Prior to any USPC parole hearing, a prisoner may request disclosure of documents to be used by the USPC in making its determination per 18 U.S.C. §4208(c); 28 CFR §2.55(a). Disclosure is limited to reports and other documents that will be used by the USPC. In some cases, disclosure can be handled by the BOP because most documents that the USPC relies upon are provided to the USPC by the BOP. The Commission may provide the prisoner's representative with a copy of the presentence report, which the BOP prohibits from disclosure to the prisoner. The USPC will withhold information designated as confidential by the sentencing court under the Federal Rules of Criminal Procedure.[7]

Additionally, a prisoner or parolee may request disclosure of information in the USPC file at other times under 28 CFR §2.56 and the FOIA. Other persons may obtain disclosure only upon proof of authorization from the prisoner or parolee or to the extent permissible under the FOIA or Privacy Act of 1974. Generally, documents in the USPC file prepared by other agencies subject to the FOIA are referred to those agencies for disclosure.[8]

---

[7] Material may be exempt from disclosure under §2.55(a) if it contains diagnostic opinions which, if known to the prisoner, could cause a disruption of his institutional program, material that would reveal a source of information obtained upon promise of confidentiality, information that may result in harm to any person as stated in 28 C.F.R. §2.55(c). If an individual's material is withheld from disclosure, the USPC will identify it, provide the exemption under which it is withheld, and summarize the information with as much specificity as possible without revealing the non-disclosable information.

[8] Documents or portions of documents may be withheld from disclosure by the USPC under an exemption from the FOIA. according to 5 USC §552(b)(1)-(9). Disclosure under this section is authorized by 28 C.F.R. §16.85 under which the USPC is exempt from the record disclosure provisions of the Privacy Act of 1974, as well as certain other provisions of that Act

Instructions on how to submit a request are provided on USPC's FOIA webpage (https://www.justice.gov/uspc/freedom-information-act-foia).

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):** July 7, 2023 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:** USPC does not have any open POAMs.
	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 FIPS categorization for OMS is Moderate. This is based on the confidentiality, integrity, and availability levels of information types contained in the system, including Criminal Incarceration, Citizen Protection, Crime Prevention, Judicial Hearings, and Legal Prosecution and Litigation.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Monitoring functions have been implemented and are conducted on a continuous basis at the external boundary of the environment, as well as within the internal network. DOJ develops and documents security assessment and authorization policy and procedures which are reviewed at least annually and updated when organizational review indicates updates are required.
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:** OMS satisfies the Audit and Accountability (AU) controls outlined by NIST,

pursuant to 5 U.S.C. §552a(j)(2).

	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA. OMS audit logs are reviewed weekly as required by DOJ policy which is formally documented in DOJ Order 0904 and the DOJ Cybersecurity Standards, Audit and Accountability (AU) Control Family.
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 related 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?

The Justice Case Access Platform (JCAP) system runs on a Windows-based, Azure.gov server platform and is made of a series of instances/modules. OMS is one of the applications within JCAP.[9] Each instance/module has accounts and requires each user to have separate single sign on logins for each account with accounts only visible to users with proper access permissions. Access control to data in the system is controlled by a detailed set of permissions which are grouped into roles. Roles are assigned to users along with assignments of accounts. DOJConnect remote access system provides the option to utilize PIV Card and RSA SecurID tokens to authenticate and provide additional integrity to remote access sessions. End users access the web application from their standard Justice Consolidated Office Network (JCON) desktop workstations using a web browser, such as Internet Explorer.

Infrastructure Operation Services (from Justice Management Division Office of the CIO) utilizes cryptography to protect the confidentiality and integrity of remote access sessions by providing secure VPN tunnels that use CISCO AnyConnect VPN Client. While the VPN supports strong encryption during transit, data is not encrypted at rest. The System Delivery Staff (SDS) within Infrastructure Operation Services is working towards encryption at rest by the end of 2022.

Infrastructure Operation Services protects the confidentiality and integrity of information while SDS performs daily backups that have error checking capabilities in conjunction with system specific virus detection software and a strict access control structure to prevent unauthorized access to each of the individual systems. The team provides all IT support for USPC. USPC will contact Application

[9] Justice Management Division Office of the CIO (OCIO) JCAP hosts four applications: Offender Management System (OMS) for United States Parole Commission (USPC), Automated Docket System (ADS) 2.0 for Office Solicitor General (OSG), Equal Employment Opportunity Application (EEOAS) for Equal Employment Opportunity (EEO).

Technical Services (ATS) with any suspected incidents. Generally, ATS follows the guidance provided in the Service Delivery Staff Incident Response Plan when managing JCAP.[10]

JCAP audit logs are reviewed weekly, by DOJ Justice Management Division (JMD) Information System Security Officer, as required by DOJ Order 0904. The audit and accountability policies and procedures are formally documented in DOJ Order 0904 and the DOJ Cybersecurity Standards, Audit and Accountability (AU) Control Family.

The security planning policy and procedures are formally documented in DOJ Order 0904, the Planning (PL) control family within the DOJ Cybersecurity Standard, and the DOJ Security Assessment & Authorization (DOJ SA&A) Handbook. DOJ Order 0904 is the primary mechanism for the Department to document its overarching IT security plan and requirements. Specific security control requirements are contained within the DOJ Cybersecurity Standard, and implemented in CSAM following procedures and guidance provided in the DOJ SA&A Handbook.

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.)

Paper records are retained in an active state for the length of parole and supervised release or pending actions. A record becomes inactive when the person is no longer on supervision and therefore no longer under the Commission's jurisdiction. In all cases inactive records will be archived within one year of inactive status. In accordance with NARA Records Schedule N1-438-98-1 and NC1-438-79-1, federal parole paper files are to be destroyed 10 years after they become inactive and D.C. Cases are to be destroyed 35 years after they become inactive. In accordance with NARA Records Schedule N1-438-00-1, data elements such as criminal records, sentencing information, hearing records, and Parole Commission decision records will be stored within the IT system permanently to facilitate FOIA requests and data analysis for recidivism. Digital records created in OMS are stored indefinitely, consistent with the applicable record schedule. Finally, in accordance with NARA Records Schedule N1-438-088-1, witness security records are retained for three years after parole termination (e.g., death, expiration of sentence, or early termination of sentence by USPC), and then transferred to Washington National Records Center, and destroyed after twenty years from the date of parole termination.

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.

[10] Application Technical Services (ATS) and Infrastructure Operation Services (IOS) are two sub offices located within Service Delivery Staff (SDS). SDS falls under JMD OCIO. OMS follow JMD OCIO's Incident Response Plan.

Records are retrieved by either name, federal inmate register number (USMS Registration Number), and/or D.C. Department of Corrections number.

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/PRC-001, *Docket, Scheduling and Control*, last published in full 52 Fed. Reg. 47182, 281 (Dec. 11, 1987).
- DOJ/PRC-003, *Inmate and Supervision Files*, last published in full 53 Fed. Reg. 7813 (Mar. 10, 1988).
- DOJ/PRC-004, *Labor and Pension Case, Legal File and General Correspondence System*, last published in full 53 Fed. Reg. 40533 (Oct. 17, 1988).
- DOJ/PRC-005, *Office Operation and Personnel System*, last published in full 53 Fed. Reg. 40535 (Oct. 17, 1988).
- DOJ/PRC-006, *Statistical, Educational, and Developmental System*, last published in full 52 Fed. Reg. 47182, 287 (Dec. 11, 1987).
- DOJ/PRC-007, *Workload Record, Decision Result, and Annual Report System*, last published in full 53 Fed. Reg. 40535 (Oct. 17, 1988).

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

Collecting more personal information than is necessary to accomplish the DOJ's official duties can be a potential threat to privacy. The USPC mitigates this privacy risk by minimizing the collection and use of Social Security numbers and implementing data access controls to OMS to ensure that the collected information is only accessed by those employees and contractors who are required to access the information to perform their official duties. OMS users cannot search for a particular individual using an SSN. USPC does not create any documents that contain full SSNs. Older documents shared by other entities with USPC may contain full SSNs. Newer documents provided by other entities generally have masked SSNs to ensure proper handling of an individual's PII. The U.S. Parole Commission is required by statute to consider all available and relevant information to make informed decisions on release and supervision of the offender. This information is used by the agency internally to make decisions.

When the Commission collects information from victims or witnesses who are part of the parole process, the Parole Commission advises victims and witnesses that they are under no obligation to provide information, but that the information may be disclosed to the offender because the offender has a statutory and due process right to know what information the Commission is considering. The victim/witness may request that their statements be kept confidential, and the Parole Commission will create a summary of their statements. The Commission will protect the identity and location of victims. If a victim believes that the Parole Commission possesses incorrect information, they may submit letters and documents for the Parole Commission's consideration. The victim may also attend the parole hearing to provide testimony disputing information that has been provided to the Parole Commission.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the Department's use of the information in the USPC OMS system include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information.

To mitigate risk associated with USPC employee misconduct or intentional or unintentional non-compliance with security controls in OMS, the Commission provides user training, and supervision. Additionally, there exists the threat of external leaks of information from offender management partners. The Parole Commission always seeks to guard against the risk that personal information on an offender, a crime victim or a witness to a crime may be inadvertently disclosed and result in harm to the offender, victim, or witness. In general, proper training is essential to preventing inadvertent disclosures of information, in addition to establishing detailed agreements with all partners that have access to data.

There is a potential risk to privacy related to the unauthorized disclosure of information maintained in OMS. This risk is mitigated by limiting access to information in the system and through training on the use of OMS. OMS has one external interface, the D.C. Criminal Justice Coordinating Council JUSTIS system. CJCC sends Alleged Violation Report data to the Parole Commission, which secures the information by use of logical and physical access controls. The Parole Commission sends CJCC notice of action data. The agencies mitigate potential risks to privacy through memoranda of understanding and web services security based on Transport Layer Security (TLS) protocol and the OMS server's enforcement of the Hypertext Transfer Protocol Secure for all traffic received or transmitted. All employees and contractors who have access to OMS are required to complete annual DOJ Cybersecurity Awareness Training (CSAT) and Records Management training. Staff also receive training on privacy responsibilities specific to the information maintained in OMS and guidance on which information in the system may be publicly disclosed or disclosed under a published routine use or statute, *e.g.*, 18 U.S.C. 4203(e)(1).

c. Potential Threats Related to Dissemination

There is a potential risk to privacy that could result from improper access and the potential unauthorized disclosure of the information within the USPC OMS system. However, security protections that authorize and limit a user's access to information within the system mitigate this risk.

Privacy risks associated with intentional or unintentional non-compliance with cybersecurity controls are mitigated through access controls and routine vulnerability scans. OMS runs on a Windows-based server platform and is made of a series of instance/modules. Users access the web application from their standard JCON desktop workstation using a web browser, such as Google Chrome. Each instance/module has accounts and requires users to have separate logins for each account they have access to. Accounts are only visible to users who have access to them. All employees have individual log in accounts supported by use of the Personal Identity Verification (PIV) card, or other DOJ approved two-factor identity verification methodology. All USPC employees and contractors who have access to OMS must sign rules of behavior with their understanding and acknowledgement of their responsibility to safeguard and protect DOJ information and information systems from unauthorized access, disclosure, and to complete PII training and adhere to all PII training and procedures.