U.S. Department of Justice

Justice Management Division (JMD)

Privacy Impact Assessment
for the

Omega Relativity Content Analytics System (ORCA)

Issued by:
John E. Thompson
JMD Senior Component Official for Privacy

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

Date approved: April 20, 2026

(May 2022 DOJ PIA Template)

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 Omega Relativity Content Analytics System (ORCA) -- a subsystem of JMD's Omega Web Repository System (OMEGA)[1] -- is a high-availability web-based system for litigation document collection and retrieval for small and large projects in DOJ. A high-availability system maintains operations using redundant fault-tolerant components and facilities, i.e. twin operational systems that either operate in parallel or in standby – for use when the twin system fails or is taken offline for maintenance. ORCA is hosted from redundant facilities located in Alexandria, VA (Primary) and Richmond, VA (Disaster Recovery Site). Each site has redundant connectivity. ORCA allows projects that do not have the budget for a dedicated document system to utilize the benefits of one without the expense of setting a system up from scratch. The ORCA subsystem assists attorneys or other professional staff acquire, organize, and analyze information collected during litigation using computer data processing, image management, and other technologies. Litigating attorneys and other professional staff can rapidly locate information and make the best use of it during investigations, litigation, and/or settlement negotiations. Remote access allows geographically dispersed teams to collaborate and review litigation materials from their desks. The basic framework is in place to allow attorneys to save and retrieve case-related documents.

The CACI Digital Forensics Lab (CDFL) platform is an independent standalone (i.e. non-networked) system also operating within the Omega General Support System. CDFL consists of a digital forensic workstation and a forensic case management tool, Lima. The digital forensic workstation and software installed on it are used to complete all forensic work requests, such as forensic imaging of electronic media, analysis of said media, recovery of any pertinent information, and generation of findings reports as requested on a case-by-case basis. Collection, maintenance, and use of this information supports DOJ's litigation and administrative functions. Department components authorized by, or covered under, the MEGA 5 contract may request these services from CACI.

This Privacy Impact Assessment has been prepared because ORCA contains personally identifiable information (PII).

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.

[1] OMEGA is covered by separate privacy documentation.

ORCA is an online web-based repository and application-hosting environment used to assist DOJ attorneys or litigation support personnel acquire, store, process, organize, and analyze critical litigation documents. It consists of commercial off the shelf e-Discovery applications and backend databases and data stores. The information maintained in the system is collected from DOJ components, opposing parties, or other entities involved in a particular matter in response to document requests or subpoenas. The information is used to support DOJ's case administration, investigative, and litigation functions. The system is maintained by CACI, a government contractor.

CDFL forensic workstation and software elements are used independently and in an isolated air-gap environment, where all data processing occurs. The air-gap environment works in such a way that the workstation is not connected to the general support system, or any other components associated with the information system. Relevant data is extracted, using digital forensic techniques, onto a Federal Information Processing Standards (FIPS 140-2)[2] validated Apricorn external hard drive. *See* https://apricorn.com.

Depending on the scope of the processing request to CACI, the data is handled in one of two ways:

(1) If CACI processes and hosts the data, the extracted data is passed over to ORCA to: review documents for relevance to claims and defenses involved in the litigation; conduct privilege reviews of documents collected in the investigation; track the use of documentary evidence in litigation; prepare witness kits/binders for depositions and hearings; link analysis relevant to litigation or investigation; and select and prepare exhibits for trial; or
(2) If CACI does not process and host the data, the extracted data is returned to the DOJ component following chain of custody requirements.

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. §§ 514-19 Federal Information Security Modernization Act of 2014
Executive Order	
Federal regulation	28 C.F.R. §§ 0.45-0.49 Subpart I – Civil Division; Federal Rules of Civil Procedure
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	MEGA 5 Contract – DOJ Contract # 15JPSS20D00000368

[2] FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module. See https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

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.

All information collected, maintained, used, or disseminated by the system is used in an effort to support DOJ's litigation and investigation functions through discovery. The information collected and stored on ORCA consists of factual case documents obtained through discovery. Depending upon the nature of the case, this information may include names, addresses, telephone numbers, and other personal information of individuals and entities from numerous sources. The information is sourced by discovery exchanges or subpoenas. The individuals may be a party to, or the subject of, DOJ litigation activities or investigations. The information collected varies based on the nature of the investigation and the documents provided via discovery.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	All information categories may apply to this system, as any of the PII of the individuals identified in column #3 can potentially be collected as part of litigation and the e-Discovery process; the collections vary on a case-by-case basis.
Date of birth or age	X	A, B, C, D	See comment above.
Place of birth	X	A, B, C, D	See comment above.
Sex	X	A, B, C, D	See comment above.
Race, ethnicity, or citizenship	X	A, B, C, D	See comment above.
Religion	X	A, B, C, D	See comment above.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	See comment above.
Tax Identification Number (TIN)	X	A, B, C, D	See comment above.
Driver's license	X	A, B, C, D	See comment above.
Alien registration number	X	A, B, C, D	See comment above.
Passport number	X	A, B, C, D	See comment above.
Mother's maiden name	X	A, B, C, D	See comment above.
Vehicle identifiers	X	A, B, C, D	See comment above.
Personal mailing address	X	A, B, C, D	See comment above.
Personal e-mail address	X	A, B, C, D	See comment above.
Personal phone number	X	A, B, C, D	See comment above.
Medical records number	X	A, B, C, D	See comment above.
Medical notes or other medical or health information	X	A, B, C, D	See comment above.
Financial account information	X	A, B, C, D	See comment above.
Applicant information	X	A, B, C, D	See comment above.
Education records	X	A, B, C, D	See comment above.
Military status or other information	X	A, B, C, D	See comment above.
Employment status, history, or similar information	X	A, B, C, D	See comment above.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	See comment above.
Certificates	X	A, B, C, D	See comment above.
Legal documents	X	A, B, C, D	See comment above.
Device identifiers, e.g., mobile devices	X	A, B, C, D	See comment above.
Web uniform resource locator(s)	X	A, B, C, D	See comment above.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Foreign activities	X	A, B, C, D	See comment above.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	See comment above.
Juvenile criminal records information	X	A, B, C, D	See comment above.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	See comment above.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, D	See comment above.
Grand jury information	X	A, B, C, D	See comment above.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	See comment above.
Procurement/contracting records	X	A, B, C, D	See comment above.
Proprietary or business information	X	A, B, C, D	See comment above.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	See comment above.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	See comment above.
- **Video containing biometric data**	X	A, B, C, D	See comment above.
- **Fingerprints**	X	A, B, C, D	See comment above.
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, D	See comment above.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- **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	Only CACI staff have administrative access to the system.
- **User passwords/codes**	X	A,	Only CACI staff have administrative access to the system.
- **IP address**	X	A,	Only CACI staff have administrative access to the system.
- **Date/time of access**	X	A	Only CACI staff have administrative access to the system.
- **Queries run**	X	A	Only CACI staff have administrative access to the system.
- **Contents of files**	X	A, B, C, D	Only CACI staff have administrative access to the system (DOJ users and third-party outside counsel have user access to cases as assigned by a case manager).
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			

Other (specify):

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	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	X	Private sector	X
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.

	How information will be shared			
Recipient	**Case-by-case**	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Mega5 staff have direct access to ORCA and CDFL to manage/administer component offerings and perform continuous monitoring of system in line with DOJ's cybersecurity requirements.
DOJ Components	X		X	DOJ litigating components requesting the ability to leverage the system within their organization will maintain direct access to the system. New users are authorized prior to use.
Federal entities	X		X	DOJ may share case/e-discovery

	How information will be shared			
Recipient	**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 and collaborate with other federal entities on a case-by-case basis, as needed.
State, local, tribal gov't entities	X		X	DOJ may share case/e-discovery information and collaborate with SLT entities on a case-by-case basis as needed.
Public	X			Some information collected and used for DOJ investigations and litigation becomes public through court proceedings, pursuant to court rules, orders, and procedures.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			DOJ may share data pertaining to e-discovery to opposing counsel or need-to-know parties for litigation purposes.
Private sector	X		X	Department contractors, including CACI employees; other parties and individuals involved in investigations and litigation, pursuant to court rules, orders, and procedures.
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.

Information processed and stored within ORCA and CDFL will not be released to the public for "Open Data" purposes or for research or statistical analysis 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.

In most cases, individuals are not provided notice prior to the collection of documents and particular uses of the information obtained through court order, warrant, subpoena, discovery requests, and other legal means. To the extent individualized notice is required by law, court rules, or DOJ policy, the Department will provide varying degrees of direct notice to individuals whose privacy interests are implicated by these orders/requests. In addition, ORCA users are provided a Privacy Act notice prior to information collection during account provisioning and also prior to each logon to the Relativity system. Generalized notice is provided pursuant to a system of records notice published in the Federal Register, as discussed in Section 7, below.

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.

Individuals do not have the opportunity to decline to provide information. Documents are obtained through court order, warrant, subpoena, discovery requests, and other legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by ORCA.

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.

See Section 5.2, above. Generally, individuals do not have opportunity to access information contained in ORCA, as the information is obtained through court order, warrant, subpoena, discovery requests, and other legal means. DOJ has generally exempted such information from the access and amendment provisions of the Privacy Act, in accordance with 28 CFR Part 16 Subpart D. An opposing party may, however, challenge the use of this information pursuant to the rules applicable to the litigation.

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 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):** ORCA: 11/03/2025 – expires on 11/3/2028, CACI-CDFL: 11/25/2024 **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:** N/A
	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:** System categorization is FIPS-199 Moderate. The system may contain PII and/or other SBU that requires protections outlined in FIPS 199 as requiring a moderate control baseline.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Completed DOJ Security Authorization. CACI administrative staff and OCIO continuously monitor applications and websites for potential misuse.
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:** This system satisfies the Audit and Accountability controls outlined by NIST 800-53A-Rev. 5, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, including formalized Audit and Accountability Policies and Procedures, technical controls, and role-based privilege separation. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA.
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: The following training is required for authorized users to access or receive information in the system:** General information security training, as well as training specific to the system for authorized users within the Department, including authorized users outside DOJ (as necessary). All DOJ employees must complete annual cyber security refresher training, insider threat training, and compliance training.

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?

ORCA: All policies, procedures, standards, and program plans for the ORCA system fully meet the security policies and requirements of the Department and FISMA. The Department defines the frequency of reviews and updates for security documents via its Security and Privacy Assessment and Authorization Handbook. Department Core Controls are assessed annually. Key information security controls employed to assure information is handled in accordance with its prescribed use including strong authentication requirements (multi-factor authentication), centralized security event management, and FIPS 140-2 validated strong encryption.

CDFL: In addition to all controls implemented for ORCA, all access to CDFL is tightly controlled by DOJ contract stipulations, DOJ security standards, and FISMA requirements. Only approved CDFL personnel, which consists of CACI Employees approved by the DOJ to work on the MEGA contract, have access to data within the CDFL. The forensic workstation is an off-line system with no internet or network access. As detailed in Section 1, all data remains encrypted on external Apricorn hard drives. The physical drives are delivered to the ORCA system team for data import or returned to the originating DOJ component.

Note that Omega has a separate PIA.

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.)

Data will be retained in ORCA until DOJ determines that the litigation materials no longer need to be stored on the system, typically after a case has closed or settled, and the information is not needed for other cases or investigations. In consultation with the component attorney assigned to the matter, the DOJ Service Delivery Staff will dispose of records that do not need to be maintained pursuant to DOJ's obligations under the Federal Records Act. Records that must be maintained will be retained in accordance with the applicable retention schedule. Archiving a case transfers the data out of the system to an external storage device, which is provided to the

attorney to file with the official record of the case.

Files managed on ORCA may include both federal records and non-records that are associated with a variety of different types of DOJ litigation case files. The retention policies for the files depend on the federal record status, as well as the classification of the type of case file to which the files pertain. The Department's record retention schedules are published at: https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. Record retentions for case files range from approximately five years to 65 years after the case close-out date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records are destroyed when no longer needed for business purposes/convenience of reference.

The CDFL performs forensic collections on devices received from DOJ components and creates images of these devices directly to FIPS 140-2 validated encrypted Apricorn drives. This data is either returned to the requesting DOJ components through chain of custody or delivered to ORCA for processing and hosting. CDFL does not collect, store, or host any collected data. Machines used to perform the forensic collection are securely wiped after each collection activity and restored to the approved baseline image.

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).

__X___ No. _____ 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:

Account, audit log, and user records maintained in this system for the purpose of monitoring system activity are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records." The digital extractions of electronic media maintained in this system for the purpose of meeting the DOJ's investigation and litigation missions are covered by the following SORNs:

- JUSTICE/ATR-001, "Antitrust Division Expert Witness File"
- JUSTICE/CIV-001, "Civil Division Case File System"
- JUSTICE/CRM-001, "Central Criminal Division Index File and Associated Records"
- JUSTICE/CRT-001, "Central Civil Rights Division Index File and Associated Records"
- JUSTICE/ENRD-003, "Environment & Natural Resources Division Case & Related Files System,"
- JUSTICE/USA-005, "Civil Case Files,"
- JUSTICE/USA-007, "Criminal Case Files,"

- JUSTICE/USA-010 "Major Crimes Division Investigative Files,"
- JUSTICE/TAX-001, "Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records,"
- JUSTICE/TAX-002, "Tax Division Civil Tax Case Files, Docket Cards, and Associated Records."

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?

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.***

There is a potential risk to privacy that could result from the improper access to information in ORCA or from retention of information in the system longer than is required by DOJ's record-keeping requirements. Security protections that authorize and limit a user's access to information within the system mitigate the risk of improper access. Physical controls, such as secured entrances and security officers, protect access to the building where the servers and workstations are located. Remote access to the system is provided by FIPS 140-2 validated transport layer security (TLS)[3] encrypted transport. All authentication utilizes government-issued personal identity verification (PIV) credentials[4] or RSA tokens[5] for outside counsel. In addition, before a user is granted authorized access to a system hosted by CIV, the user completes required security training, including cybersecurity training and privacy training specific to the user's role. Individuals outside DOJ are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access accounts. In

[3] TLS provides privacy and data integrity between two communicating applications. TLS ensures that the connection between two communicating applications is encrypted. See https://csrc.nist.gov/glossary/term/transport_layer_security.
[4] A PIV card is a card issued to an individual that stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials. https://csrc.nist.gov/glossary/term/personal_identity_verification.
[5] RSA tokens display a passcode that a user may use to authenticate to a system. RSA tokens are used to implement two-factor authentication.

addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Information access to the system is granted on a need-to-know basis. Case managers and the lead attorney grant limited system access to DOJ attorneys, other DOJ professional staff, other federal employees, and contractors for the cases/matters those personnel work on, not the entire system

There are monitoring and auditing tools for each system to review user activity. As a result, JMD can monitor user access within the system. Access controls are backed up by detailed audit logs that provide a detailed overview of how data has been accessed and used within the system to ensure compliance with applicable handling policies. In addition, the system generates detailed metadata and audit logging information that can help administrators manage data retention schedules as established for the system. Data can be identified based on its age, the specific case that it is supporting, whether the data remains in active use, and other parameters that might be relevant to a data retention decision. JMD follows Department internal policies and procedures for unauthorized access or release of information from the system.

In addition to these protections, all disk volumes and backup tapes containing PII or other Sensitive But Unclassified Information (SBU) are encrypted via a hardware-based encryption mechanism in compliance with FIPS140-2, Security Requirements for Cryptographic Modules. In addition, ORCA and CDFL employ intrusion detection and prevention systems to detect and prevent potential malicious activity, changes to the network, and traffic anomalies. Further, ORCA backs up data regularly and controls access to data stored on the applications through the aforementioned mechanisms. Frequent network and system vulnerability scanning are designed to ensure all vulnerabilities and associated risks are addressed and mitigated in a timely manner. A combination of access, logical, and technical controls provide a robust suite of policies, procedures, and technology that ensure PII and other SBU are protected at all points in the ORCA and CDFL systems.