United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for the
USAVault System (USAVault)

Issued by:
Senior Component Official for Privacy - Kevin S. Krebs

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

Date approved: May 21, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

USAVault System is an enterprise data storage system which provides a data storage and data backup solution that supports the mission and daily operations for the United States Attorney's Offices (USAO). The system offers data management and security, and serves as a central repository for USAO agency data.

The USAO consists of 94 districts with offices spread across the continental United States, Alaska, Hawaii, Guam, Puerto Rico, and the U.S. Virgin Islands. The USAO also includes the Executive Office for the United States Attorneys (EOUSA). Headquartered in Washington, DC, the EOUSA performs management and liaison functions for the USAO.

The primary datacenter is the Network Operations Center (NOC) located in in Columbia, SC. The site houses the USAVault servers and equipment. The alternate site is located at the Core Enterprise Facility – TX (CEF-TX) Data Center in Richardson, TX, which houses contingency or failover servers for the NOC.

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.

USAVault is the data storage infrastructure that supports both the mission and the daily operations of the USAO. USAVault is accessible to all USAO/EOUSA authorized personnel and is used to process, store, and transmit USAO information in support of the mission to enforce federal laws.

The data types stored in USAVault include investigation and litigation materials collected through issuance of civil investigative demands, search warrants, subpoenas, and discovery requests. These materials may contain a variety of PII about members of the public, including personal contact information, date of birth, and employment information. They may also contain medical or health information, tax identification numbers, and other sensitive information, if relevant to a particular matter.

USAVault also processes, stores, and transmits internal human resources information, which may contain personal contact information, date of birth, social security numbers, employment history and performance ratings, and, if relevant, medical or health information. EOUSA Office of the Chief Information Officer, Enterprise End User Technologies (OCIO/EEUT) Staff and/or District IT staff are responsible for the administration, operation, and management of USAVault functional services.

There are various major and minor applications that use or link to USAVault, and these can include PII as it relates to financial, healthcare fraud, civil and criminal law enforcement

applications, internal administrative applications, and other legal evidence. All systems using USAVault services will require the completion of an Initial Privacy Assessment for those systems by the business owner responsible for that system and any associated applications and system data.

Districts are responsible for managing the district data stored in USAVault. District administrators have full access to the data belonging to that district within USAVault and have the rights to store, delete, or change their data within USAVault. District users require formal approval and authorization to access information for each case and can access only the data that they are authorized to access.

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

Authority	Citation/Reference
Statute	• 5 U.S.C. § 301 • 28 U.S.C. § 547 • 28 U.S.C. Ch. 35 • 44 U.S.C. Chs. 21, 25, 27, 29, 31, and 33
Executive Order	
Federal regulation	• 28 C.F.R. Part 16
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	• DOJ ORDER 0904, Cybersecurity Program (September 15, 2016) • DOJ ORDER 0908, Use and Monitoring of DOJ Information Technology, Information Systems, and Access to Authorized Users' Electronic Information (August 18, 2020)

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 - NonUSPERs	(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 and D	
Date of birth or age	X	A, C and D	
Place of birth	X	A, C and D	
Sex	X	A, C and D	
Race, ethnicity, or citizenship	X	A, C and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, C and D	SSNs are collected for DOJ personnel. SSNs may also be included in case information from outside entities, although SSNs are not actively collected or requested.
Tax Identification Number (TIN)	X	A, C and D	
Driver's license	X	A, C and D	
Alien registration number	X	A, C and D	
Passport number	X	A, C and D	
Mother's maiden name			
Vehicle identifiers	X	A, C & D	
Personal mailing address	X	A, C and D	
Personal e-mail address	X	A, C and D	
Personal phone number	X	A, C and D	
Medical records number	X	A, C and D	
Medical notes or other medical or health information	X	A, C and D	
Financial account information	X	A, C and D	
Applicant information	X	A, C and D	
Education records		A, C and D	
Military status or other information	X	A, C and D	

Employment status, history, or similar information	X	A, C and D	The collection of this group of information will include business addresses.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, C and D	
Certificates	X	C and D	
Legal documents	X	C and D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C and D	
Foreign activities	X	C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	
Whistleblower, e.g., tip, complaint, or referral	X	C and D	
Grand jury information	X	C and D	Access to Grand Jury information collected is limited to authorized users.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Access to this information is limited to authorized users.
Procurement/contracting records	X	C and D	
Proprietary or business information	X	C and D	
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- Photographs or photographic identifiers	X	C and D	
- Video containing biometric data	X	C and D	
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			

- Voice recording/signatures	X	C and D	
- Scars, marks, tattoos	X	C and D	
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
System admin/audit data:	X	A	USAVault is operated and administered by DOJ government and contractor personnel.
- User ID	X	A	All administrators are provided unique user IDs.
- User passwords/codes	X	A	All administrators use unique passwords and Personal Identification Verification (PIV) cards issued in accordance with HSPD-12.[1]
- IP address	X	A	IP address information is contained within the system.
- Date/time of access	X	A	Access logs with date and time of access are maintained within the system and are generally limited to the user and administrators.
- Queries run	X	A	Query runs are maintained within the system and are generally limited to the user.
- Contents of files	X	A	Contents of all files are available to administrators; otherwise access to files are limited by district.
Other (please list the type of info and describe as completely as possible):	X	C and D	Additional personal information could be collected or received through investigations and litigation.

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	✓

[1] All administrators use unique passwords and PIV cards issued in accordance with HSPD-12.

Phone	✓	Email	✓		
Other (specify):					

Government sources:					
Within the Component	✓	Other DOJ Components	✓	Other federal entities	✓
State, local, tribal	✓	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	✓		
Other (specify):					

Non-government sources:					
Members of the public	✓	Public media, Internet	✓	Private sector	✓
Commercial data brokers	✓				
Other (specify):					

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	✓		✓	EOUSA/USAO will share information among EOUSA/USAO offices on a case-by-case basis. EOUSA/USAO generally will provide access to data via EOUSA/USAO account permission setting upon Section Chief/Assistant Chief approval. The requester's access is limited to only authorized data.

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	✓			EOUSA/USAO will share USAVault information with other DOJ components on a case by-case basis. EOUSA/USAO generally will share data via encrypted documents though email or via the USAFX system upon Section Chief/Assistant Chief approval. The requester's access will be limited to the requested data once the recipient's need to know has been verified. Both the data that can be accessed and the duration of access to the data will be at on the data owner or case manager's discretion, consistent with law and policy.
Federal entities	✓			EOUSA/USAO will share USAVault information with other DOJ components on a case by-case basis. EOUSA/USAO generally will share data via encrypted documents though email or via the USAFX system upon Section Chief/Assistant Chief approval. The requester's access will be limited to the requested data once the recipient's need to know and authority to share the data has been verified. Both the data that can be accessed and the duration of access to the data will be at on the data owner or case manager's discretion, consistent with law and policy.

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.**
State, local, tribal gov't entities	✓			EOUSA/USAO will share USAVault information with other DOJ components on a case by-case basis. EOUSA/USAO generally will share data via encrypted documents though email or via the USAFX system upon Section Chief/Assistant Chief approval. The requester's access will be limited to the requested data once the recipient's need to know and authority to share the data has been verified. Both the data that can be accessed and the duration of access to the data will be at on the data owner or case manager's discretion, consistent with law and policy.
Public	✓			While records are generally not provided directly to members of the public, records submitted to courts are generally publicly available according to court rules.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	✓			Some of the data stored within USAVault may be shared with counsel, parties, witnesses, or courts as part of the litigation process, at the direction of the AUSA managing the case.

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.**
Private sector	✓			EOUSA/USAO will share USAVault information with private sector on a case by-case basis for an authorized purpose. EOUSA/USAO generally will share data via encrypted documents though email upon Section Chief/Assistant Chief approval. The requester's access will be limited to the requested data. Both the data that can be accessed and the duration of access to the data will be at on the data owner or case manager's discretion.
Foreign governments	✓			EOUSA will share USAVault information on a case-by-case basis with foreign governments once the recipient's need to know and authority to share the data has been verified.
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.

EOUSA provides only statistics and case filings to the "Open Data" site (www.data.gov). EOUSA's public case filings may properly contain PII.

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.

EOUSA/USAO provides generalized notice to the public regarding the collection and maintenance of personal information through the publication of SORNs. A full list of EOUSA/USAO SORNs is available at this link: https://www.justice.gov/opcl/doj-systems-records#USA. All USA SORNs apply to USAVault given that USA Vault may contain information from across all of EOUSA/USA's system of records. Additionally, the following Department-wide SORNs SORNs are all applicable to USAVault:

- JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records (formerly Department of Justice Computer Systems Activity and Access Records), last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), 82 Fed. Reg. 24147 (May 25, 2017), and 86 Fed. Reg. 37188 (July 14, 2021).
- JUSTICE/DOJ-005, Nationwide Joint Automated Booking System (JABS) last published in full at 71 FR 52821 (9-07-2006) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-007, Reasonable Accommodations for the Department of Justice last published in full at 67 FR 34955 (5-16-2002) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-011, Access Control System (ACS)last published in full at 69 FR 70279 (12-03-2004) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-013, Justice Federal Docket Management System [Justice FDMS] last published in full at 72 FR 12196 (3-15-2007) and modified at 82 FR 24151, 153 (5-25-2017) and 85 FR 15227 (3-17-2020).

For information related to personnel actions and other activities not related to law enforcement activities, individuals are also provided with a Privacy Act Section (e)(3) notice at the time of collection when collecting information directly from the individual.

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.

There are limited opportunities for individuals to participate in the collection, use, and dissemination of information stored in USAVault associated with the civil and criminal investigations and litigation. Individuals have greater opportunities to participate in the collection, use, and dissemination of personal information related to personnel actions and other activities not related to law enforcement activities. Generally, such information collected from individuals is done so on a voluntary basis. However, the refusal to provide such information, in certain circumstances, may result in the individual's inability to perform the functions of their duties (e.g. information needed for human resources, employment, and performance functions).

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 information stored in USAVault that is associated with the law enforcement investigations and litigation are not subject to amendment, and individuals may have limited access rights. For example, the subject of an investigation would not necessarily be afforded notice, access, and amendment to such information during the course of the investigation.

For information related to personnel actions and other activities not related to law enforcement activities, individuals may request access to and amendment of their records by visiting the USAO website for making a Privacy Act/FOIA request: 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. (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):** On 1/30/2023, USAVON storage assets were split from USAVON and assigned a new ATO – USAVault. The ATO for USAVault was granted on 10/12/2023, and expires on 10/12/2026. **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:** A POAM was created to track the completion of the IPA and PIA.
	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:** In accordance with procedures defined within NIST Special Publication 800-60 Volume II Revision 1, USAVault has been assigned a Security Categorization of **Moderate** based on the type of information processed, stored, and transmitted within its boundaries.

X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** USAVault has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. All system documentation supporting these activities are maintained within the Department's Joint Cybersecurity Assessment and Management system (JCAM).
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:** All logs are reviewed weekly by system ISSO and then gathered and centrally managed using the Department's audit analysis solution, SPLUNK. All logs are forwarded to the Security Operations Center (SOC) for automated analysis and review.
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:** All EOUSA users are subject to onboarding training that includes computer security awareness and privacy training. This training is also required annually by the DOJ department.

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?

All USAVault users are required to use multi-factor authentication to access the system. Data access is highly restricted: users require formal approval and authorization to access information for each case and can access only the data that they are authorized to access. All users are required to undergo training and sign formal Rules of Behavior prior to being granted access to data in USAVault.

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 in the USAVault system is maintained for as long as it is needed by the authorized DOJ users. The data is subject to the respective retention periods that govern the data, e.g., NARA General Records Schedules, agency SF-115s, and any applicable SORNs published under the Privacy Act of 1974, 5 U.S.C. §552a (see https://www.justice.gov/opcl/doj-systems-records). Procedures have been developed to ensure that electronic copies are not retained beyond the retention period established for the original records and will be disposed in accordance with

DOJ Network Account Records Management USAPP No. 3-13.300.004.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

EOUSA/USAO provides generalized notice to the public via a collection of SORNs. A full list of EOUSA/USAO SORNs is available at this link: https://www.justice.gov/opcl/doj-systems-records#USA. All USA SORNs apply to USAVault given that USA Vault may contain information from across all of EOUSA/USA's system of records. Additionally, the following Department-wide SORNs SORNs are all applicable to USAVault:

- JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records (formerly Department of Justice Computer Systems Activity and Access Records), last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), 82 Fed. Reg. 24147 (May 25, 2017), and 86 Fed. Reg. 37188 (July 14, 2021).
- JUSTICE/DOJ-005, Nationwide Joint Automated Booking System (JABS) last published in full at 71 FR 52821 (9-07-2006) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-007, Reasonable Accommodations for the Department of Justice last published in full at 67 FR 34955 (5-16-2002) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-011, Access Control System (ACS)last published in full at 69 FR 70279 (12-03-2004) and modified at 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147) and 82 FR 24147 (5-25-2017).
- JUSTICE/DOJ-013, Justice Federal Docket Management System [Justice FDMS] last published in full at 72 FR 12196 (3-15-2007) and modified at 82 FR 24151, 153 (5-25-2017) and 85 FR 15227 (3-17-2020).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

The privacy risks associated with information collected within USAVault primarily relate to the loss of confidentiality, integrity, and availability of data. Access by unauthorized entities to sensitive data, including personal information collected for investigations or litigation, potentially could lead to destruction of that data, compromised identities, exposure of sensitive and personal data, and/or disruption to an ongoing investigation or litigation.

USAVault is a EEUT Internal system. EOUSA uses a number of proven protection methods, including secure communications (e.g., JUTNET, JCOTS), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques designed to ensure data is protected to the extent possible and in accordance with DOJ Secure Configuration Guidelines and IT security standards.

EOUSA adheres to DOJ continuous monitoring requirements, including encryption for data at rest. For example, any PII data saved locally to an EOUSA laptop is protected at rest by FIPS compliant encryption technology. Second, EOUSA assesses DOJ defined core controls annually and all controls at least every three years. Finally, EOUSA adheres to the OIG schedule for routine FISMA assessment.

Additionally, all data collected within USAVault is protected by encryption planning to be fully implemented by 2026, and is viewable only by authorized individuals, who must authenticate and be given direct permission for each dataset. All user activity is monitored and audited based on user actions and accesses. USAVault internal user management module manages user access and only allows users the ability retrieve data based on each user authorized role and rights.

Furthermore, to avoid over-collection, data collected is associated with authorized user identities. Only the necessary data for each user is collected, preventing the over-collection of unnecessary or excessive data. Tailored Data Collection: By linking data collection to specific user identities, the system can gather only the data relevant to that particular user. This reduces the likelihood of collecting general data that may be irrelevant to a specific user. Access Control and Privacy: Since the data is associated with a specific authorized user, this allows for tighter control over who has access to which data. It limits the scope of data collection to what's strictly necessary for that user's interaction or experience. This also aligns with privacy regulations, which emphasize the collection of only the data needed for a specific purpose.

Other data is processed within other system boundaries that reside within the USAVault, will create their own system PIA. Additionally, EOUSA provides privacy notices through system of records notices (SORNS), published on DOJ's system of records website (https://www.justice.gov/opcl/doj-systems-records), and PIAs (https://www.justice.gov/opcl/doj-privacy-impact-assessments).

Finally, DOJ provides annual privacy training, in addition to the Computer Security and Awareness Training (CSAT), required of all personnel. Furthermore, privacy specific analysis and reporting is maintained within an authorized DOJ JCAM profile. The capability to

generate reports from USAVault is controlled by permissions and limited to authorized personnel in support of the USAVault system.