United States Department of Justice

Justice Management Division

Privacy Impact Assessment
for the
DOJ Veritone aiWARE

Issued by:
Morton J. Posner
Senior Component Official for Privacy

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

Date approved: March 19, 2025

(May 2019 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 Department of Justice (DOJ) Justice Management Division (JMD) Veritone aiWARE system is a Federal Risk and Authorization Management Program (FedRAMP) authorized Software-as-a-Service (SaaS) used to support the DOJ components in accelerating the processing and analysis of audio, video, and text-based multimedia content. The SaaS is hosted within the FedRAMP authorized Infrastructure-as-a-Service, Amazon Web Services (AWS) GovCloud. JMD is not a user of the application but provides enterprise and contract administrative services to DOJ component users.

Veritone aiWARE is an artificial intelligence (AI) technology tool that analyzes multimedia and biometric information to derive meaningful connections from uploaded data and records. Once data is ingested, it is processed within Veritone aiWARE to identify and extract the desired metadata, including text, faces, locations, objects, sentiments, logos, and keywords. After content has been processed, the Veritone aiWARE suite of AI applications enables users to organize, manage, search, and analyze the data.

JMD prepared this Privacy Impact Assessment because Veritone aiWARE will collect, use, and maintain personally identifiable information (PII). Due to the nature of data collection and processing, various types of PII will potentially be a part of gathered evidence in support of authorized investigations.

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.

DOJ is responsible for, among other tasks, enforcing the law, defending the interests of the United States according to the law, seeking just punishment for those guilty of unlawful behavior, and ensuring fair and impartial administration of justice for all Americans. As part of these responsibilities, DOJ components represent the United States Government in most domestic and foreign courts, grand jury proceedings, and in administrative and adjudicative fora. DOJ components must ingest, search, analyze, and produce large amounts of data relevant to support DOJ litigation, discovery, or disclosure of document requests, as mandated by law and DOJ policy.

In support of these mission parameters, DOJ has purchased and deployed Veritone aiWare to provide components with a tool for aiding in the authorized review and analysis of evidentiary

data. Veritone aiWARE incorporates artificial intelligence technology that provides rapid extraction of actionable intelligence from large amounts of data.

This PIA covers the Veritone FedRAMP suite of tools which includes Automate, Illuminate, Redact and aiWARE. These tools support the overall evidentiary data review by the case team to transcribe, translate, and analyze video, audio, and text evidence. Additionally, Veritone aiWARE provides functionality to redact PII of individuals and sensitive items within audio, video, and image-based evidence, and perform object detection across audio, video, and text-based files within Relativity, which is a common tool in use by DOJ case teams.

The Veritone internal workspaces can be provisioned for a specific project and/or user to ensure access is limited to the identified users who have been granted appropriate access protocols. Components can utilize this feature to separate case data and limit access only to staff with a need-to-know. All data is digital and is securely uploaded through DOJ provided secure communication channels and trusted internet connections. Components are asked to implement and manage an instance of Veritone within their JCAM inventory. Their instance will be specifically tailored with the controls necessary to document and ensure protection of the types of data uploaded, processed, and, stored within the Veritone aiWARE boundary. All data must conform to the Moderate protection level defined by the Veritone aiWARE FedRAMP certification. Components will also be required to complete separate privacy documentation for each instance of Veritone.

The level of human oversight needed varies by use case. For example, if a user were bulk transcribing phone calls for the purpose of searching for responsive content by keywords or phrases, there would be little to no human oversight required to correct the AI transcription results since the accuracy of each individual word is not as important as identifying the right phone call recordings to review. However, if a user were redacting body-worn camera footage to protect the privacy of individuals before release (e.g., as part of a public records request), users have the opportunity and flexibility to review and correct the AI redaction results as needed to ensure full parity between redactions applied against identified individuals. This functionality also serves as a safeguard in the review process (i.e., ensuring individual's faces are not unwittingly exposed).

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	5 U.S.C. § 301 (agency operations) 28 U.S.C. § 516 (conduct of litigation) 28 U.S.C. § 534 (acquisition, preservation, and exchange of identification records and information; appointment of officials) 28 U.S.C. § 547 (duties of United States Attorneys)
	Executive Order	
x	Federal Regulation	28 C.F.R. Chapter 1

	Agreement, memorandum of understanding, or other documented arrangement	
x	Other (summarize and provide copy of relevant portion)	Federal Rules of Criminal Procedure Federal Rules of Civil Procedure Federal Rules of Evidence Federal Rules of Appellate Procedure Justice Manual

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.

Any PII relevant and necessary to Department litigation, investigations, e-discovery, and disclosure activities could potentially be maintained in this system, including PII not otherwise noted in the chart below. The following, non-exhaustive chart contemplates a variety of PII which may be maintained in Veritone aiWARE.

(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	
Date of birth or age	X	A, B, C, D	
Place of birth	X	A, B, C, D	
Gender	X	A, B, C, D	
Race, ethnicity or citizenship	X	A, B, C, D	
Religion	X	A, B, C, D	
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	
Tax Identification Number (TIN)	X	A, B, C, D	
Driver's license	X	A, B, C, D	
Alien registration number	X	A, B, C, D	
Passport number	X	A, B, C, D	
Mother's maiden name	X	A, B, C, D	

(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
Vehicle identifiers	X	A, B, C, D	
Personal mailing address	X	A, B, C, D	
Personal e-mail address	X	A, B, C, D	
Personal phone number	X	A, B, C, D	
Medical records number	X	A, B, C, D	
Medical notes or other medical or health information	X	A, B, C, D	
Financial account information	X	A, B, C, D	
Applicant information	X	A, B, C, D	
Education records	X	A, B, C, D	
Military status or other information	X	A, B, C, D	
Employment status, history, or similar information	X	A, B, C, D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	
Certificates	X	A, B, C, D	
Legal documents	X	A, B, C, D	
Device identifiers, e.g., mobile devices	X	A, B, C, D	
Web uniform resource locator(s)	X	A, B, C, D	
Foreign activities	X	A, B, C, D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	
Juvenile criminal records information	X	A, B, C, D	
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, D	
Grand jury information	X	A, B, C, D	
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	
Procurement/contracting records	X	A, B, C, D	
Proprietary or business information	X	A, B, C, D	
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	
Biometric data:	X	A, B, C, D	
- **Photographs or photographic identifiers**	X	A, B, C, D	
- **Video containing biometric data**	X	A, B, C, D	
- **Fingerprints**	X	A, B, C, D	
- **Palm prints**	X	A, B, C, D	

(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
- **Iris image**	X	A, B, C, D	
- **Dental profile**	X	A, B, C, D	
- **Voice recording/signatures**	X	A, B, C, D	
- **Scars, marks, tattoos**	X	A, B, C, D	
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, D	
- **DNA profiles**	X	A, B, C, D	
- **Other (specify)**			
System admin/audit data:	X	A	System maintains system logs and other audit data on system and user activity.
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Any other PII relevant and necessary to Department litigation, investigations, e-discovery, and disclosure activities could potentially be maintained.

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	X
Phone	X	Email	X		
Other (specify): Data can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including directly from the individual to whom the information pertains.					

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

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): Data can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including other government sources such as public records.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Data can be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including non-government sources.					

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	X	X	JMD will have direct access to Veritone aiWARE to manage/ administer component offerings and perform continuous monitoring of system in line with DOJ's cybersecurity requirements.
DOJ Components	X	X	X	DOJ litigating components requesting the ability to leverage the system within their organization will maintain direct access to the system. JMD must authorize new users, prior to use.
Federal entities	X			DOJ may share case/e-discovery information and collaborate with other federal entities on a case-by-case basis, as needed.

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	X			DOJ may share case/e-discovery information and collaborate with state, local, tribal, or territorial, entities on a case-by-case basis as needed.
Public	X			DOJ may release information to the public in response to a FOIA or Privacy Act request by a member of the public.
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. Any data shared would be in the form of an exported report, rather than providing system access to an outside party.
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.

Information processed and stored within DOJ Veritone aiWARE 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.

The Veritone aiWARE system can be used in a wide variety of information management projects. As such, the information at issue will be collected and maintained under a variety of

potential applicable authorities. Information maintained in Veritone will likely be part of a law enforcement investigation or judicial proceeding and therefore may be exempted from the notice provisions of the Privacy Act. However, if the information, (either orally or written), being solicited from an individual for collection or use in Veritone, is about that individual, and will become part of a system of record, and is not covered by a Privacy Act exemption, the Department provides the required 5 USC 552a(e)(3) notice to such individuals prior to collecting their information. This would include, for example, information about DOJ personnel users of Veritone.

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.

The Veritone aiWARE system can be used in a wide variety of information management projects. As such, the information at issue will be collected and maintained under a variety of potential applicable authorities. If, for example, the information at issue is law enforcement sensitive information the disclosure of which could result in danger to law enforcement personnel, the person to whom the information pertains may not be able to consent to collection or specific uses of such information. If, however, the information is such that it is not sensitive and not, for example, collected as part of a law enforcement investigation or subject to Privacy Act exemptions, the Department may be able to provide the opportunity to individuals to consent to specific uses of such information.

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 Veritone aiWARE system can be used in a wide variety of information management projects. As such, the information at issue may be collected and maintained under any of a variety of potential applicable authorities. Depending on the particular use(s), individuals will follow the access and amendment procedures in the applicable SORN(s). Individuals may also follow the procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations. The records contained in Veritone aiWARE, however, may be subject to certain exemptions to the access and amendment procedures, as articulated in the applicable SORNs, above, and in Subpart E, Part 16, Title 28, Code of Federal Regulations.

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): 10/07/2021 – 10/07/2024. **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO completed on: 09/27/2024; Expires on: 09/27/2027. **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:** POA&M 43921 has been opened to document lack of an approved PIA. This POA&M is currently in a delayed state. A milestone has been updated to reflect status.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The Veritone aiWARE FedRAMP package was reviewed by the OCIO Cybersecurity Staff (CSS). The cloud service provider, Veritone, is responsible for securing and enforcing identified security controls and informing the DOJ of any incidents.
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:** Specified audit log events tied to system are recorded and reviewed monthly by the cloud service provider using their SIEM tool and alerts/detections they have created.
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**. The Veritone aiWARE cloud services have been provided under a DOJ BPA to all Components. This BPA has included standard language to ensure contractor compliance with DOJ and Federal acquisition standards to include information security and privacy protection measures. Additionally, Veritone aiWARE is a FedRAMP approved product that also requires the vendor to verify compliance with Federal standards, policies and laws.
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:** Prior to authorizing use of the system, DOJ will require users to undergo training directly from Veritone to learn proper functionality of the software and avoid improper use.

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?

Veritone aiWARE has a security categorization of FISMA moderate based on the defined NIST 800-60 information types and current component usage. JMD and component users have assessed and implemented all applicable security controls to ensure protections commensurate with the impact to the Department from any unauthorized access or disclosure of information. Use of Veritone aiWARE for information or information systems categorized as HIGH pursuant to NIST SP 800-60 v.2 rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, is prohibited, unless all required HIGH security controls are implemented prior to such use.

A full security control assessment of the DOJ Veritone aiWARE system has been completed, and the FedRAMP package produced by Veritone goes into depth on the hosting infrastructure and controls implemented by the vendor. The principle of least privilege is enforced through privileged user accounts and non-privileged accounts that will not have administrative rights. Users are also only able to operate the system on government furnished equipment and while connected to the DOJ network, which requires users to log in using multi-factor authentication (PIV and PIN).

All data-at-rest and in-transit is encrypted compliant with the Federal Information Processing Standard (FIPS)140-2[1] validated encryption modules. A periodic review of role-based access audit logs will be done to detect any potential unauthorized access.

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.)

Veritone will host data from a variety of different source systems, therefore records retention schedules will be determined by the source system. Data will be retained in Veritone until the materials no longer need to be stored on the system. Typically, this occurs after a case has closed or settled and the information is no longer needed. Data custodians within components are responsible for determining when and which data can be destroyed.

The Component program or case managers will need to work with their SCOPs to ensure data retention within their specific instance is compliant with applicable NARA records schedule(s), and other records management requirements for the specific data being processed. Veritone online storage is configured to comply with license/contract storage agreements.

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

[1] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/publications/detail/fips/140/2/final.

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:

Below are the applicable System of Records Notices (SORNs):

- DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 132 (July 14, 2021.
- DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), and amended at 82 Fed. Reg. (May 25, 2017)

The records created, compiled, and maintained in this system to accomplish the Department's investigations, litigation, and discovery functions, may also be covered by the Department's litigation and general leadership case file SORNs, including:

- ATR System of Records Notice JUSTICE/ATR-001, Antitrust Division Expert Witness File, last published in full at 54 Fed. Reg. 42060, 061 (Oct. 13, 1989), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- BOP System of Records Notice JUSTICE/BOP-001, Prison Security and Intelligence Record System, last published in full at 67 Fed. Reg. 41449 (June. 18, 2002), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- CIV System of Records Notice JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- NSD System of Records Notice JUSTICE/NSD-001, Foreign Intelligence and Counterintelligence Records System, last published in full at 72 Fed. Reg. 26153 (May 8, 2007), and amended at 82 Fed. Reg. 24151 (May 25, 2017)

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.***

Veritone's aiWARE Government system has undergone internal & external security and compliance testing. Veritone aiWARE is only authorized for use regarding information and information systems categorized as MODERATE pursuant to NIST SP 800-60 v.2 rev. 1, The system is FedRAMP authorized at a moderate impact level based upon thorough testing by an accredited third-party assessment organization. This annual activity includes manual control testing against the NIST 800-53, penetration testing, and vulnerability assessment. Monthly, Veritone conducts continuous monitoring activities including vulnerability scanning and dynamic application security testing. Veritone's Software Development Lifecycle (SDLC) includes manual and automated mechanisms to test security and functionality of the application including static code analysis. FedRAMP assessment results and continuous monitoring content is available to DOJ in OMB MAX.gov.[2] Veritone meets with DOJ policy liaison and component representatives monthly to answer questions, provide clarity around deliverables, and discuss when any updates to the software will be made. When a new component is scheduled to be deployed to the system's boundary, Veritone will update the security assessment plan (SAP) which will be tested during the annual third-party assessment.

As indicated in the table within section 3.1, all types of information up to the MODERATE categorization (no HIGH information) will potentially be stored within DOJ Veritone given the nature of litigation materials and e-discovery. The main potential privacy risks associated with this system and the data that is being stored and processed is: (1) unauthorized access, (2) unauthorized disclosure or breach of PII, and (3) data over-collection, including use of Veritone to process information categorized as HIGH pursuant to NIST SP 800-60 v.2 rev. 1.

To mitigate these risks, only cleared DOJ personnel that have a need-to-know, with DOJ network accounts and email addresses, will have authorized access to this system using two-factor authentication (PIV card and PIN). Litigating components that require use of this system will need to authorize the system internally with their designated risk/authorizing official prior to use within their environment. To enforce need-to-know requirements, components will then have a separate instance created so they only have access to documents managed by their respective component, and users within each component will be further restricted to access only those matters to which they are assigned. Further, all users of Veritone receive training on proper disclosure of sensitive information.

To further mitigate privacy risks resulting from the sensitive information, including PII, maintained in Veritone aiWARE, JMD has implemented numerous security controls, consistent with Section 6, above. For instance, Veritone aiWARE is a FedRAMP authorized SaaS solution. The FedRAMP is a standardized security assessment and authorization process for cloud products and services used by the

[2] OMB Max.gov is a government-wide suite of advanced collaboration, information sharing, data collection, publishing, business intelligence and authentication tools and services used to facilitate cross-government collaboration and knowledge management. In this case, the FedRAMP document repository is being referred to.

U.S. federal agencies. As a result, Veritone aiWARE was reviewed by an authorized third-party assessment organization and has been authorized to operate by the Department of Justice's authorizing official. A DOJ authority-to-operate (ATO) was granted after an assessment and documentation of NIST Special Publication 800-53, Rev 5 security and privacy controls have been implemented.

To further safeguard information maintained in Veritone aiWARE, all data at rest, including backups, are encrypted with Storage Service Encryption, which is deemed to be FIPS 140-2 validated. Data in transit, which is both internal and external web traffic, is encrypted as well using Transport Layer Security (TLS) 1.2.[3] The Information Security System Officer and system stakeholders will meet with the cloud service provider, Veritone, periodically to perform continuous monitoring of security controls and any changes that may occur. Veritone has incident response procedures that include preparation, detection and analysis, containment, eradication, and recovery, as well as collaboration/notification of DOJ. An annual system contingency plan and incident response tabletop exercise will be performed in accordance with continuous monitoring guidance.

To mitigate the risk of data over-collection, the users that are a part of the litigating components are trained to perform e-discovery in a manner that is intended to identify and collect only information relevant to the litigation matter at hand. Additionally, components using Veritone will train all users on the requirements to only use Veritone for information and information systems categorized pursuant to guidance in NIST SP 800-60 v.2 rev. 1, as MODERATE and below.

By Department policy, all DOJ users (federal and contractor) with access to Department networks, must complete annual Cyber Security Assessment Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.

---

[3] The "Transport Layer Security" protocol is used "to secure communications in a wide variety of online transactions . . . . Any network service that handles sensitive or valuable data, whether it is personally identifiable information (PII), financial data, or login information, needs to adequately protect that data." NIST, Special Publication 800-52, rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.