United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for
DOJ Enterprise Endpoint Detection and Response (EDR) Cloud

Issued by:
Morton J. Posner
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: May 21, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Department of Justice (DOJ) Enterprise Endpoint Detection and Response (EDR) - Cloud (DOJ Enterprise EDR - Cloud) solution is designed to secure networked computer systems at the endpoint.[1] DOJ employs a suite of tools, services, and integrated technologies from CrowdStrike[2] to provide advanced cybersecurity threat protection and response, next-generation anti-virus, threat intelligence/hunting, and advanced cyber hygiene practices for the Department, as well as External Federal Agencies (EFA) subscribers.

The DOJ Enterprise EDR - Cloud system is comprised of three connector services - Application Programming Interface (API), Telemetry, and Web services. To deploy the system, there are two primary hardware (or virtual equivalent) components - servers and sensors.

Capabilities include:

- Next-Generation Anti-Virus - Next-Generation Antivirus (NGAV) uses a combination of behavioral detection, machine learning algorithms, and exploit mitigation, so known and unknown threats can be anticipated and immediately prevented.
- Asset Discovery – Designed to identify unmanaged assets within the organizations network that lack the CrowdStrike agent. This feature is limited to a component's network infrastructure where CrowdStrike is deployed and does not engage in monitoring or collecting data from external networks or workstations.
- Endpoint Detection and Response – The endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
- Threat Intelligence – Enables system owner teams to make faster, more informed, data-backed security decisions.
- Threat Hunting – The practice of proactively searching for evidence or indicators of active cyber threats in the environment that have slipped past the initial endpoint security defenses.
- IT Hygiene Assessment – Enables improved visibility into DOJ and government customer networks to identify vulnerabilities and provide additional protections before breaches occur.
- Restful APIs – Enables analysts and incident response administrators to interact with the system through scripts, commands, or offline procedures.
- Web Console – Provides JMD authorized privileged users of the EDR-Cloud access to a majority of system administration functions required for management of CrowdStrike.
- Real-Time-Response Capabilities – Allow extraction of logs needed by analysts when analyzing Indicators of Compromise (IOCs) in monitored systems.
- Streaming API of Events – Used to send logs to Splunk[3] for ingestion and use by the Splunk CrowdStrike application.
- Falcon Data Replicator (FDR) Services – serves as storage within an Amazon Web Services (AWS) S3 (cloud data storage) bucket.
- Flight Control – Enables DOJ to manage users' and sub-components' access by defined roles.

---

[1] Terminology that refers to a device or computing system (e.g. laptop, workstation, or server) that is connected to a network. Each interconnected device or computing system is considered an endpoint on the network.
[2] https://www.crowdstrike.com/en-us/.
[3] Splunk is covered by separate privacy documentation here: https://www.justice.gov/opcl/media/1363231/dl?inline.

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.

The DOJ Enterprise EDR-Cloud collects and maintains cybersecurity focused information related to endpoint vulnerability data, security events, and system activities. The information is captured from connected endpoints on DOJ, DOJ Components', and external federal agency customers' networks. The information is aggregated and stored in EDR-Cloud to support security posture checking, security event analysis, incident response, and event remediation/mitigation efforts.

To monitor and manage the EDR-Cloud platform, privileged user accounts will be maintained in the system. These accounts will have varying degrees of privileges in the system to either: maintain and configure the EDR-Cloud platform; or maintain and configure tenant resources hosted on the EDR-Cloud platform. The account profiles for these users will include business e-mail addresses, primarily to establish contact and communications with the user. These e-mail addresses are also attributable to specific DOJ Component employees or contractors, or external federal customer employees or contractors.

EDR-Cloud platform monitoring and collection activities will capture audit, access, and security logs from EDR-Cloud system operations' activities. These logs will contain privileged user account logins, time/data of access, IP addresses of remote login hosts, system IDs of remote login hosts (often attributable to a specific user's computer), and system activities performed on EDR-Cloud platform, i.e., Privileged Operations, including:

- Account Management events;
- Policy Changes;
- Activities requiring elevated privilege;
- System events;
- System alerts;
- System failures;
- System process execution events, process tracking, and detection (where possible); and/or
- Access alerts for critical system files, environment files, executables, or library (objects).

EDR-Cloud log monitoring and system auditing shall include: all attacks and indicators of potential attack, privileged operations, unauthorized access attempts (local or network), and system alerts/failures. These log messages as configured, implemented, and managed by Cloud Engineering for GovCloud and the Commercial Cloud, as well as IT for internal systems, shall contain enough information to ensure:

- What type of event occurred;
- When the event occurred;
- Where the event occurred;
- The source name (i.e., host) of the event;
- The outcome of the event; and
- The identity of any individuals or subjects associated with the event, limited to the individual's email and workstation that was affected by a vulnerability. Each workstation has a unique identifier, which is tied to an individual. (Traceability can be completed by EDR-Cloud Analysts or Administrators.)

Event Logging is continuous and includes:

- Successful and unsuccessful account logon; and
- Authentication and authorization events associated with access connections.

The capabilities of the EDR-Cloud security operations center (SOC) include:

DOJ Justice Security Operations Center (JSOC) analysts, investigating an event, have the ability to track down device(s) affected by a vulnerability. This includes access to a user's email address provided for registration to the CrowdStrike console. In addition, user log on/off sessions and user information, associated with events, could be captured. Quarantined files relating to an incident are automatically sent to a JMD Falcon console (a siloed Web-based user interface dashboard) for further investigation. Quarantined files on an infected machine are accessible by a JMD Tier 3 or 4 analyst in the context of an investigation. Component-level permissions are required before Tier 3 or 4 JMD analysts can make threat factor determinations on files and investigate file contents, which may contain PII.

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	Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3541 *et seq.* Federal Information Technology Acquisition Reform Act of 2014, 40 U.S.C. §§ 11101-11704.
Executive Order	Executive Order (EO) 14028, "Improving the Nation's Cybersecurity"
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	DOJ's Office of the Chief Information Officer (OCIO) has entered into a memorandum of understanding with each EFA.
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A & B	Audit logs may contain first and last names of system users (i.e., individuals associated with EDR-Cloud the system accounts)
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A & B	The DOJ Enterprise EDR - Cloud security monitoring features and/or endpoints/host systems monitored by the EDR-Cloud contain device identifiers such as an Asset ID, Computer name, Media Access Control (MAC) address, Host Groups, Active Directory domain, Serial Number, City, which is often attributable to DOJ Component Employees, Contractors or other Federal Government Personnel.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			

(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
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & B	i) DOJ Enterprise EDR - Cloud platform – privileged users that monitor and manage the system or tenant resources – access and security logs contain admin user ID, IP addresses, data/time of access, and system activities; and ii) EDR security monitoring features – endpoint/host systems monitored by EDR – captured access and security log information contains endpoint login user ID, IP address, system ID (often attributable to a specific user), data/time of access, and system activities.
- **User passwords/codes**			
- **IP address**	X	A & B	i) DOJ Enterprise EDR - Cloud platform – privileged users that monitor and manage the system or tenant resources – access and security logs contain admin user ID, IP addresses, data/time of access, and system activities; and ii) EDR security monitoring features – endpoint/host systems monitored by EDR – captured access and security log information contains endpoint login user ID, IP address, system ID (often attributable to a specific user), data/time of access, and system activities.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- **Date/time of access**	X	A & B	i) DOJ Enterprise EDR - Cloud platform – privileged users that monitor and manage the system or tenant resources – access and security logs contain admin user ID, IP addresses, data/time of access, and system activities; and ii) EDR security monitoring features – endpoint/host systems monitored by EDR – captured access and security log information contains endpoint login user ID, IP address, system ID (often attributable to a specific user), data/time of access, and system activities.
- **Queries run**			
- **Contents of files**	X	A, B, C, and D	Privileged users have the ability to access the contents of files on DOJ endpoints, including files that hold PII of DOJ employees or third parties, but will do so only in the course of a cybersecurity investigation, accordance with DOJ policy. i) DOJ Enterprise EDR - Cloud platform – privileged users that monitor and manage the system or tenant resources – access and security logs contain admin user ID, IP addresses, data/time of access, and system activities; and ii) EDR security monitoring features – endpoint/host systems monitored by EDR – captured access and security log information contains endpoint login user ID, IP address, system ID (often attributable to a specific user), data/time of access, and system activities.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, & D	DOJ Enterprise EDR - Cloud platform security monitoring features – ability to capture network connection, session, and IP on end-points for threat analysis and response – IPs could be traced back to insider and external threat actor network hosts and devices which has the potential to be attributable to a person.

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	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
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	X		X	JMD OCIO CSS JSOC analysts, JMD OCIO CSS JSOC CTAT Threat Hunt Team, JMD OCIO CSS JSOC Engineering, as well as members of the DOJ Insider Threat Program, have direct access to this system. Other entities within JMD receive access to such information on a case-by-case basis (for example, as part of incident response efforts).
DOJ Components	X		X	Component personnel have access to their component's Crowdstrike deployment.
Federal entities	X		X	JMD OCIO CSS JSOC analysts, JMD OCIO CSS JSOC CTAT Threat Hunt Team, JMD OCIO CSS JSOC Engineering, as well as members of the DOJ Insider Threat Program, have direct access to this system. The JMD EDR-Cloud provides Security Operations Center, Endpoint Protection Platform Management, Justice Edge Services, and Security Information and Event Monitoring for External Federal Agencies. The EFA's are all considered managed clients of the DOJ JMD EDR-Cloud. The JMD EDR-Cloud Incident Response team, on a case-by-case basis, does share incident information with these clients as well as provides support for remediation and mitigation of security related events in support of remediation and mitigation of an incident related to the EFA's.

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				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			As required by Law and after conferring with appropriate legal counsel. For instance, sharing with Congress. In the event a critical security event occurs, JMD may be required to share the security event. An example of this was the July 19th, 2024 Crowdstrike misconfiguration security event. As mentioned above, the JMD does not actively share security event information unless they are required to do so by Law on a case-by-case basis.

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.

DOJ Enterprise EDR-Cloud information will not be released to the public for "Open Data" 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.

DOJ users are provided with a warning banner prior to accessing DOJ endpoints. As follows:

Notice to Users

You are accessing U.S. Government information technology and/or information systems which includes: (1) this information technology, (2) this information system, (3) all information technology devices connected to this network, and (4) all devices and storage media attached to this information system or to information technology on this network.
This information technology and information system is provided for U.S. Government-authorized use only. You have no reasonable expectation of privacy when using this information technology and/or information system and the government may monitor, intercept, search and/or seize data transiting through or stored within. Unauthorized or improper use may result in disciplinary action as well as civil and/or criminal penalties.

Individuals are notified that accounts, audit logs, and user records, maintained in DOJ Enterprise EDR - Cloud and used to manage system services, are covered by JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021); and JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 Fed. Reg. 41089 (July 30, 2021).

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.

No such opportunity exists. The DOJ Banner explains that individuals will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to DOJ Enterprise EDR-Cloud administrators.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals are notified that accounts, audit logs, and user records, maintained in DOJ Enterprise EDR - Cloud and used to manage system services, can be accessed or amended in accordance with 28 C.F.R. Part 16, Subpart D, and in accordance with JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021); and JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 Fed. Reg. 41089 (July 30, 2021).

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).

	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): March 20, 2024 (Ongoing Authorization – no expiration/renewal date due to continuous assessment review cycles) **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:**
X	Outstanding POA&M associated with NIST 800-53 Rev 5 control RA-8, Privacy Impact Assessments.
	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:
	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:
X	The Enterprise EDR – Cloud has been categorized as a 'High.' Factors considered for the categorization include the systems capabilities to access information made available at a given endpoint which the systems capabilities are deployed at. The confidentiality of the endpoint information is deemed as 'High.'
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
X	CrowdStrike Falcon GovCloud Platform is FedRAMP authorized, under FedRAMP's primary governing body the Joint Authorization Board, Software as a Service (SaaS) offering for federal customers. The FedRAMP assessment was completed by a Third-Party Organization which enables the CrowdStrike Falcon GovCloud Platform to operate under a FedRAMP authorization. The DOJ Enterprise EDR – Cloud is provided to the DOJ Justice Management Division (JMD) as a SaaS solution by the CrowdStrike Falcon GovCloud Platform vendor. All activities related to testing and/or evaluation are inherited from the vendor by the DOJ JMD. Monitoring of both physical and logical information systems and assets is also inherited from the vendor by the DOJ JMD as there are no associated hardware or software which the DOJ JMD is responsible for maintaining for the EDR-Cloud SaaS. The DOJ Logging as a Service (DOJ LaaS)[4] JMD system provides the DOJ Enterprise EDR –

[4] Logging as a Service (LaaS) is covered by separate privacy documentation here: https://www.justice.gov/opcl/media/1363231/dl?inline.

	Cloud with application layer audit and event monitoring capabilities which are limited to user level event monitoring (Logging in and logging out, unsuccessful login attempts by assigned users, monitoring of all application layer actions performed by the user within the EDR-Cloud). The assigned Information System Security Officer (ISSO) additionally performs continuous monitoring of the system through weekly audit log reviews for unsuccessful login attempts and annual security control assessments.
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:** The DOJ Enterprise EDR – Cloud is provided to the DOJ Justice Management Division (JMD) as a Software as a Service (SaaS) by the vendor CrowdStrike Falcon GovCloud Platform. All activities related to testing and/or evaluation are inherited from the vendor by the DOJ JMD. Monitoring of both physical and logical information systems and assets is also inherited from the vendor by the DOJ JMD. The DOJ Logging as a Service (DOJ LaaS) JMD system provides the DOJ Enterprise EDR – Cloud with audit and event monitoring capabilities for all associated system users. Audit events which require further investigation are escalated to the DOJ JMD Security Operations Center (JSOC).
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 DOJ users are required to complete Cyber Security Awareness Training (CSAT), DOJ-OPCL-CS-011, General Privacy Training (2024), as well as read and agree to comply with DOJ information technology Rules of Behavior both prior to accessing the DOJ network, and annually thereafter. System administrators, including DOJ Enterprise EDR – Cloud Administrators, must complete additional professional training, which includes security 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?

A full security control assessment has been completed for DOJ Enterprise EDR – Cloud to include, but not limited to, physical access, logical access, identification, authentication, vulnerability management, and audit. The DOJ Enterprise EDR – Cloud makes use of separate privileged and non-privileged user accounts. For privileged (i.e., system administrator) accounts, the system leverages additional role-based access control technologies that allow for administrator session recording.

All application log data is sent to DOJ's centralized audit log management system for triage and review. The DOJ Enterprise EDR – Cloud system utilizes Transport Layer Security

encryption to secure information across network communications between the DOJ EDR-Cloud sensor and the Cloud Service Provider. This is compliant with the Federal Information Processing Standards Publication (FIPS) 140-25, to protect data in transit through TLS encrypted end to end certificate pinned connections. In addition, DOJ Enterprise EDR – Cloud inherits network security and use of the CrowdStrike Falcon GovCloud vendor's Application Layer Firewall, which integrates intrusion detection systems (IDS)/intrusion prevention systems (IPS) technology to protect inbound and outbound communications. The CSS Information Security Systems Officers (ISSO's) are charged with reviewing logins and performing auditing functions to ensure role-based access controls are satisfying the above measures.

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.)***

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 3.2, for records created and maintained by Federal agencies related to protecting the security of information technology systems and data and responding to computer security incident. Log data is maintained in Logging as a Service as the DOJ's repository for 365 days. See 64 FR 73585 (12-30-1999).

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:

JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (7-14-2021), 2021-14986_-_doj-002_sorn_update.pdf (justice.gov) and;

JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 Fed. Reg. 41089 (July 30, 2021).

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.***

Information Collected, Purpose, and Benefit to DOJ:
EDR-Cloud collects and maintains cybersecurity focused information related to endpoint vulnerability data, security events, and system activities. The information is captured from connected endpoints on DOJ, DOJ Components, and external federal agency customers' networks. The information is aggregated from security logs and events and stored in EDR-Cloud to support security posture checking, security event analysis, incident response, and event remediation/mitigation efforts. Security and event logs could include names, personal e-mail addresses, personal phone number, and device identifiers. Primarily, EDR collects and maintains endpoint vulnerability data, cyber-attack details, indicators of comprise, privileged operations, unauthorized access attempts (local or network), and system alerts/failures, security events, and system activities.

To monitor and manage the EDR-Cloud platform, privileged user accounts will be maintained in the system. These accounts will have varying degrees of privileges in the system to either: maintain and configure the EDR-Cloud platform; or maintain and configure tenant resources hosted on the EDR-Cloud platform. The account profiles for these users will include business e-mail addresses, primarily to establish contact and communications with the user. These e-mail addresses are also attributable to a specific DOJ, DOJ Component, or external federal customer employee or contractor.

EDR-Cloud platform monitoring and collection activities will capture audit, access, and security logs from EDR-Cloud itself. These logs will contain privileged user account logins, time/data of access, IP addresses of remote login hosts, system IDs of remote login hosts (often attributable to a specific user's computer), and system activities performed on EDR-Cloud platform, i.e. Privileged Operations, including: account management events, policy changes, and any other activity requiring elevated privileges.

Privacy Risks:
There are certain privacy risks associated with the collection, use, access, dissemination, and maintenance of the PII that is collected. Some potential risks are identity theft, blackmail, physical harm, discrimination, and emotional distress.

Mitigations:
The DOJ LaaS ingestion of EDR-Cloud logs for monitoring and system auditing shall include: all attacks and indicators of potential attack, privileged operations, unauthorized access attempts (local or network), and system alerts/failures. Log messages shall contain enough information to ensure

collection of:

- what type of event occurred;
- when the event occurred;
- where the event occurred;
- the source of the event;
- the outcome of the event; and the identity of any individuals or subjects associated with the event, limited to the individual's email (workstation or endpoint that was affected by a vulnerability. Each workstation has a unique identifier, which is tied to an individual. Traceability can be completed by EDR-Cloud Analysts or Administrators).

Event Logging is continuous and includes:

- successful and unsuccessful account logons; and
- authentication and authorization events (connection events).

The DOJ Justice Enterprise Event Streaming System (JEESS)[5] tool acts as a data minimization and log reduction tool when moving applicable audit data to the DOJ LaaS Indexers and does not store any data. The DOJ Enterprise EDR-Cloud does not seek or request certain data sensitive types from its users (such as Social Security Numbers and Tax Identification Numbers) to minimize the collection of PII, although such data may be ingested.

By Department Order, all DOJ users with access to Department networks, including DOJ Enterprise EDR-Cloud, must complete an annual Cybersecurity Awareness Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the 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 established 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.

Data Retention:
Audit log and Data retention is fully managed by the DOJ JMD Secure Enclave system[6], which is the hosting site for the DOJ LaaS and includes 12 months of active storage and 18 months of cold data storage once the 12 month storage limit is reached.

Specific uses or sharing:
Component-level permissions are required before Tier 3 or 4 analysts can make threat factor determinations on files and investigate file contents, which may contain PII. The DOJ Enterprise EDR - Cloud shares Investigative, Configuration Management, Threat Management, and Endpoint and Threat tuning on a case by case basis within the JMD component amongst the JMD OCIO CSS JSOC

---

[5] Justice Enterprise Event Streaming System (JEESS) is covered by separate privacy documentation here: https://www.justice.gov/opcl/media/1390011/dl?inline.
[6] Secure Enclave is covered by separate privacy documentation here: https://www.justice.gov/JMD_Secure_Enclave_PIA/dl?inline.

Watchfloor analysts (Tier, 1, 2, and 3), JMD OCIO CSS JSOC CTAT Threat Hunt Team, and the JMD OCIO CSS JSOC Engineering. The JMD EDR-Cloud provides Security Operations Center, Endpoint Protection Platform Management, Justice Edge Services, and Security Information and Event Monitoring for External Federal Agencies. The EFA's are all considered managed clients of the DOJ JMD EDR-Cloud. The JMD EDR-Cloud Incident Response team, on a case-by-case basis, shares incident information with these clients as well as provides support for remediation and mitigation of security related events in support of remediation and mitigation of an incident related to the EFA's.

- ***Privacy notices to individuals***

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. The DOJ Banner explains that individuals will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to DOJ Enterprise EDR-Cloud administrators. Individuals are notified that accounts, audit logs, and user records, maintained in DOJ Enterprise EDR - Cloud and used to manage system services, are covered by JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021); and JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 Fed. Reg. 41089 (July 30, 2021).

- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

To ensure data and privacy protections are relevant and effective, security controls and risk assessments (including privacy and security control assessments) are routinely evaluated. In accordance with the NIST Special Publication 800-53 Rev 5, these assessments include management, operational, and technical controls to ensure minimization of any privacy risk.