Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Secure Enclave

Issued by:
Arthur E. Gary
JMD General Counsel and Senior Component Official for Privacy

Approved by: Peter Winn, Chief Privacy and Civil Liberties Officer (Acting), Department of Justice

Date approved: May 14, 2020]

(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 Secure Enclave is an unclassified computing environment that provides security, flexibility, and enhanced contingency capability for the Department of Justice (DOJ) Information Security Continuous Monitoring (ISCM), Identity, Credential, and Access Management (ICAM) tools and services, and for applications hosted by the Justice Security Operations Center (JSOC). These tools and services include, but are not limited to, authentication and identity management, virtualization and hosting technology, vulnerability management, and network-based threat detection tools. [1]

The DOJ has implemented Secure Enclave as a hosting environment for tools, services, and applications only. Secure Enclave administrators will have access to the full range of administrative and system management information for the tools, services, and applications hosted on Secure Enclave. In such a situation, Secure Enclave administrators may have access to information accessible to the tool, service, and/or application users. If the tool, service, or application maintains personally identifiable information (PII), the Secure Enclave administrators would also have access to that information. Given the potential for administrators' information access to information about individuals other than government employees and contractors, JMD has prepared a Privacy Impact Assessment (PIA) for this system.

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 Justice Management Division (JMD) Cybersecurity Services Staff (CSS) supports and secures the DOJ and its components by providing cybersecurity leadership across the Department. The Secure Enclave hosts CSS tools, services, and applications that protect and preserve the confidentiality, integrity, and availability of DOJ's electronic information. To support the DOJ mission, Secure Enclave hosts applications that provide network and endpoint management, incident response, information assurance, identity and access management, and tools for insider threat detection and response.

To securely host these tools, services, and applications, CSS requires a secure set of system resources that operate in the same security domain and share the protection of a single, common, continuous

[1] The tools, services, and applications hosted by the Secure Enclave will have their own privacy compliance document, as required by applicable privacy laws, regulations, and policies, including but not limited to DOJ Policy and the Federal Information Security Modernization Act of 2014 (FISMA). See Section 8 regarding privacy risks and mitigation.

security perimeter—known as an "enclave."[2] The Secure Enclave is an infrastructure that enables the Secure Enclave administrators and the tool, service, and application users to perform cybersecurity functions in a secure, highly available, and segmented[3] computing environment. The specific information that is collected, handled, disseminated, stored, or accessed within the Secure Enclave suite of tools, services, and/or applications will be assessed for each, respectively. The tools that are hosted in the Secure Enclave will inherit certain security controls implemented and assessed under this PIA.

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, Pub. L. 113-283, 128 Stat 3073; 40 U.S.C. 1441 note, requiring Federal Agencies to plan for the security and privacy of their computer systems
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	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.

[2] *See, e.g.*, Committee on National Security Systems Instruction No. 4009, Glossary (April 6, 2015), https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[3] The term "segmented" refers to the Secure Enclave environment separated by firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) (further described in Footnote 9), and managed exclusively by Secure Enclave administrators.

(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 and B	For system audit/administration purposes
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	X	A and B	Personnel may incidentally share personal e-mail addresses rather than DOJ e-mail addresses.
Personal phone number	X	A and B	Some personnel are not issued government GFEs
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			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A and B	Government cell phone information only, for system audit/administration purposes
Web uniform resource locator(s)			
Foreign activities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges			
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**			
- **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:	X	A and B	
- **User ID**	X	A and B	
- **User passwords/codes**	X	A and B	
- **IP address**	X	A and B	
- **Date/time of access**	X	A and B	
- **Queries run**	X	A and B	
- **Content of files accessed/reviewed**	X	A and B	
- **Contents of files**	X	A and B	

(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 (See Comments)	A, B, C, D (See Comments)	Secure Enclave administrators will have access to the full range of administrative and system management information for the tools, services, and applications hosted on Secure Enclave. Secure Enclave administrators may have access to information stored and processed in the application. The tools, services, and applications hosted on Secure Enclave that collect, process, disseminate, and store PII will detail such in separate privacy compliance documentation.

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		Online	X
Phone		Email	X	Other	X
Other (specify): Individuals will directly provide, or systems will automatically collect, user profile information, contact information, and other PII necessary and relevant to the respective tools, services, and applications hosted on Secure Enclave.					

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): Some of the tools, services, and applications hosted on the Secure Enclave are offered to other Federal Government agencies. These Federal Government agency customers may source information maintained on the system.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): The tools, services, and/or applications hosted on Secure Enclave may be provided from private-sector service vendors. In such case, some information may be sourced from the service vendor.					

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	System administration/audit as needed to ensure operability of Secure Enclave tools, in accordance with Section 6, below. Information may be shared within the component on a case-by-case basis (for example, as part of incident response efforts).
DOJ Components	X			Information may be shared to other DOJ components on a case-by-case basis (for example, as part of incident response efforts).
Federal entities	X			Information may be shared to other Federal entities on a case-by-case basis (for example, as part of incident response efforts).
State, local, tribal gov't entities				N/A
Public				N/A

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				N/A
Private sector	X			Information may be shared to the Department's private sector service vendors, on a case--specific basis, for system administration, including but not limited to, tool, service, and/or application troubleshooting.
Foreign governments				N/A
Foreign entities				N/A
Other (specify):	X			As required by law.

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.

Secure Enclave 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.

Individuals have been notified that the account, audit log, and user records maintained in Secure Enclave, and the tools, services, and applications hosted on Secure Enclave, to plan and manage system services are covered by are JUSTICE/DOJ-002, 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), and 82 Fed. Reg. 24151,

153 (May 25, 2017). [4]

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.

Secure Enclave Administrators will have access to the full range of administrative and system management information for the tools, services, and applications hosted on Secure Enclave. In such a situation, Secure Enclave administrators may have access to information accessible to the tool and service application users for the purpose of system administration, maintenance, and continuity. Individuals will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to Secure Enclave 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 have been notified that the account, audit log, and user records maintained in Secure Enclave, and the tools, services, and applications hosted on Secure Enclave, to plan and manage system services can be accessed or amended, in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002, 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), and 82 Fed. Reg. 24151, 153 (May 25, 2017).

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 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): **6/25/2019**
	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:

[4] With regards to Section 5, other notices and procedures to allow individuals access to information in the system pertaining to them may apply, depending on the nature of information maintained in the tools, services, and/or applications, and how the information is retrieved. The tools, services, and/or applications hosted by the Secure Enclave will have their own privacy compliance document, as required.

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: **The Secure Enclave has vulnerability and configuration scans completed monthly.**
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: **Logs are collected daily.**
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 must complete computer security awareness training annually, 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 Secure Enclave 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 the Secure Enclave, to include physical and logical access, identification and authentication, vulnerability management, auditing, and other assessment actions to ensure that security controls are operating as intended. The Secure Enclave makes use of separate Privileged and Non-Privileged user accounts and leverages additional role based access control technologies and administrator session recording. All system and application log data is being sent to DOJ's centralized audit log management system for triage and review. The Secure Enclave makes use of Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2,[5] to protect data in transit between the browser and the user's workstation,[6] makes use of Application Layer Firewall[7] and integrated Intrusion Detection System / Intrusion Prevention System[8] technology, and encapsulates in an Internet Protocol

[5] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/groups/STM/cmvp/standards.html.
[6] A User Workstation is intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems.
[7] An "Application Layer" firewall is a form of firewall that controls input, output, and/or access from, to or by an application or service.
[8] An Intrusion Detection System (IDS) analyzes and monitors network traffic for signs that indicate attackers are using a

Security Virtual Private Network (IPSEC VPN)[9] all data replication/transit between the two Secure Enclave datacenters. The CSS Information Security System Officers (ISSOs) are charged with reviewing logins and performing auditing functions to ensure role-based access controls satisfy 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 incidents. 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).

__ 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:

DOJ-002, 64 FR 73585 (12-30-1999), as modified by 66 FR 8425 (1-31-2001) and 82 FR 24147 (5-25-2017).[10]

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

known cyber threat. Intrusion Prevention System (IPS) proactively denies network traffic based on a security profile if that packet represents a known security threat.

[9] Internet Protocol Security, or "IPSEC," is "a framework of open standards for ensuring private communications over public networks, and is "typically used to create a virtual private network." NIST SP 800-77, *Guide to IPsec VPNs* (Dec. 2005). A Virtual Private Network, or "VPN," is a "virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks." *Id.*

[10] With regards to Section 7, other published Government-wide and DOJ System of Records Notices may apply, depending on the nature of information maintained in the tools, services, and applications, and how the information is retrieved. See, e.g., JUSTICE/DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 FR 60110 (Nov. 7, 2019). The applications hosted by the Secure Enclave will each have privacy compliance documentation, including SORNs, as required.

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

The Secure Enclave hosts tools, services, and applications that may collect PII, and those systems may collect other sensitive systems operation information to include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of actions, queries run, contents of files). JMD's collection and use of PII, as described here and throughout this PIA, may create certain privacy risks. To mitigate these risks, all data retention is managed according to System Owner requirements and associated policies. Data minimization strategies including data retention is determined on the tool, service, or application level. The Secure Enclave does not collect certain data types for its users (such as Social Security Numbers and Tax Identification Numbers) to minimize the collection of PII.

Additionally, sources of information come directly from the users (government and contractors), systems automatically collecting information, and from external government sources such as other Federal Government agencies where applications hosted on the Secure Enclave are offered as a service. To further mitigate any risks associated with these activities, the Secure Enclave implements encryption, account management and access controls, auditing, and system monitoring tools to mitigate and protect privacy information. The Secure Enclave makes use of separate Privileged and Non-Privileged user accounts and access is granted based on least privilege and need-to-know requirements. DOJ users (government and contractors) will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to Secure Enclave Administrators.

Information is shared on a case-by-case basis within the component, other DOJ Components, other Federal agencies, and the private sector (for vendor-specific system troubleshooting), and via direct login by the Secure Enclave administrators. To further mitigate any risks associated with these activities, the Secure Enclave uses encryption and logging controls for mitigation purposes. The Secure Enclave makes use of Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2, to protect data in transit between the browser and the user's workstation, makes use of Application Layer Firewall and integrated IDS/IPS technology, and encapsulates in an IPSEC VPN all data replication/transit between the two Secure Enclave datacenters. The Secure Enclave ISSO performs continuous

monitoring of the security controls within the system to ensure security protections are operating as intended.

By Department Order, all DOJ users with access to Department networks, including Secure Enclave, must receive an 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.

Finally, to ensure the continued relevance and effectiveness of security controls, risk assessments, including privacy and security control assessments are routinely evaluated. In accordance with the NIST Special Publication 800-53 (Rev.4), these assessments includes the management, operational, and technical controls to ensure minimization of any privacy risk.