U. S. Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Email Security Platform Cloud (ESP-Cloud)

Issued by:
Morton J. Posner
JMD General Counsel and Senior Component Official for Privacy

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

Date approved: April 29, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Department of Justice (DOJ or Department) Cybersecurity Services Staff (CSS) enters into agreements to provide information technology services to external federal government agency customers. As part of these agreements, DOJ employs the Email Security Platform - Cloud (ESP-Cloud). ESP-Cloud is a cloud-based email security solution designed to provide inbound and outbound email security including antivirus and anti-spam (AV/AS) protection. ESP-Cloud provides the Justice Security Operations Center (JSOC) with the ability to perform email monitoring, specifically the ability to monitor email traffic to and from External Federal Subscriber networks for malicious activity or security threats.

ESP-Cloud scans inbound and outbound email traffic for malicious activity, such as viruses. If ESP-Cloud detects suspected security threats, it generates an alert, makes the contents of email and any associated data viewable, and can quarantine mail identified as malicious or spam. In addition, it collects email meta-data such as sending email server IP address, sender email address, recipient email address, subject, and attachment name. This information is stored in the ESP-Cloud system (for 30 days) and copied to the DOJ's Logging as a Service[1] cloud for permanent storage based on retention schedule.

JSOC security staff and External Federal Subscriber (Read Only accounts) may review these security alerts and related data in the ESP-Cloud console and investigate whether a security incident occurred (called threat analysis). The Designated Signing Official (DSO) approves certain members of the JSOC security staff administrative access to ESP-Cloud. Any JSOC security staff administrators must have a valid "need to know" basis for their approval.

DOJ prepared this Privacy Impact Assessment because ESP-Cloud will collect, use, and maintain personally identifiable information (PII).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

---

[1] DOJ's Logging as a Service (LaaS) uses Splunk to collect, store, query, and correlate machine logs. As a result of LaaS capturing these actions, the application can generate graphs, reports, and alerts in support of the Department's audit logging and monitoring. LaaS is covered by separate privacy documentation. *See* https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.

DOJ Cybersecurity Shared Services provides services to External Federal Subscribers and is a separate instance from what DOJ uses for itself. Part of these services include the ESP Cloud information system. This service provides monitoring to the External Federal Subscribers to include:

- Inbound and outbound email security including antivirus and anti-spam (AV/AS) protection.
- ESP-Cloud enables auto-remediate for Office 365 to remove emails that become malicious after delivery.
- Attachments are detonated in a virtual sandbox against various operating systems, applications, and web browsers to identify malicious behavior.
- Advanced URL Defense feature provides detection of malicious URLs embedded in an email message and can prevent a user from accessing these malicious URLs.
- Leverages intelligence about attacks and bad actors to prioritize alerts and block threats in real time.
- Retroactively analyzes and alerts when an email becomes malicious post-delivery.

The ESP-Cloud system team deploys the Trellix primary secure email gateway (SEG) with "Full Hygiene," a set of vendor security features enabled to provide comprehensive protection against various email threats including advanced malicious files, malicious universal resource locator (URL), i.e. website, checks, and sophisticated impersonation and business email compromise (BEC) attacks. In this deployment model, incoming emails from the Internet are forwarded to the Trellix Email Security Cloud, where the emails are scanned, analyzed, quarantined if suspected/identified as malicious, and system administrators receive alerts. Emails determined to be safe for delivery are forwarded to the customer for end user delivery. Trellix administrators manage alerts or release emails via Trellix Email Security Cloud portal. The ESP-Cloud system establishes two main roles assigned to administrators, a general administrator role (release quarantine e-mails, update policy configurations, etc.) and a read-only role (query e-mail events and read policies).

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 (FISMA), 44 U.S.C. §§ 3551, *et seq.* Federal Information Technology Acquisition Reform Act of 2014 (FITARA), 40 U.S.C. §§ 11315, *et seq*.
Executive Order	Executive Order 14028 – Improving the Nation's Cybersecurity
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	CSSP Memorandum of Agreement (MOA) with each External Federal Subscriber

Other (summarize and provide copy of relevant portion)	DOJ Order 0904, Cybersecurity Program

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.

Email messages may include significant quantities of personal information relating to substantive work of External Federal Subscribers. Because email messages maintained in ESP-Cloud could conceivably include almost any type of unclassified PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. Therefore, the items of information checked below are limited to end-user information and log information maintained by ESP-Cloud.

(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	Names are required for account creation. ESP-Cloud could also collect this information if included in an email.
Date of birth or age			
Place of birth			
Sex			
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			

(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			
Personal mailing address			
Personal e-mail address	X	A, B, C and D	ESP-Cloud could collect this information if included in an email
Personal phone number			
Business e-mail address	X	A, B	Business email addresses are required for account creation. ESP-Cloud could also collect this information if included in an email.
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	X	A, B	ESP Cloud could collect legal documents in materials scanned and included in an email
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	A, B	ESP Cloud could collect legal documents in materials scanned and included in an email
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			

(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
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, B	Admin audit log data is collected
- **User ID**	X	A, B	Admin audit log data is collected
- **User passwords/codes**	X	A, B	Admin audit log data is collected
- **IP address**	X	A, B	Admin audit log data is collected
- **Date/time of access**	X	A, B	Admin audit log data is collected
- **Queries run**	X	A, B	Admin audit log data is collected
- **Contents of files**	X	A, B	Admin audit log data is collected
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	ESP-Cloud could collect other data not identified above if this information is included in an email

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Information could be collected if an External Federal Subscriber is corresponding with government entities.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Information could be collected if an External Federal Subscriber is corresponding with non-governmental entities.					

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	The cloud-based email security solution is designed to provide inbound and outbound email security including antivirus and anti-spam (AV/AS) protection and email monitoring for the External Federal Subscriber and is separate from the solution DOJ deploys to protect itself. Information may include the following: date and time of email, subject, sender and recipient email addresses, body of email and attachments (if email identified as

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**
				SPAM or malicious), and email header.
DOJ Components	X			Information sharing with another DOJ Component will only occur upon request from the External Federal Subscriber who owns the information or by order of an authorized investigatory or judicial process.
Federal entities	X			Information sharing with other federal entities will only occur upon request from the External Federal Subscriber who owns the information or by order of an authorized investigatory or judicial process. Information may include the following: date and time of email, subject, sender and recipient email addresses, body of email and attachments (if email identified as SPAM or malicious), and email header, when such sharing is relevant to the investigation of a security incident (e.g., with an individual or entity whose information was involved in the incident).
State, local, tribal gov't entities	X			Information sharing with State, local, tribal government entities will only occur upon request and/or with consent from the External Federal Subscriber who owns the information. Any sharing of information would be based on a legitimate need and be governed by an information sharing agreement.
Public				

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	X			Information sharing will only occur upon request and/or consent from the External Federal Subscriber who owns the information or by order of an authorized investigatory or judicial process, on a case-by-case basis.
Private sector	X			Information may be shared with the ESP Cloud vendor, on a case-specific basis, for system administration, including but not limited to, tool, service, and/or application troubleshooting.
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 in ESP Cloud will not be released to the public for "open data" 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.

A warning banner notifies external federal users that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in such information. Relevant sections from the DOJ Rules of Behavior include six primary topics on Notice, Consent, and Access:

- No Expectation of Privacy

- Collection of Personally Identifiable Information (PII)
- Access and Use of PII
- Maintenance of PII
- Disclosure of PII
- Data Breach

Individuals are also provided general notice that email traffic is monitored and records maintained with the ESP Cloud systems services are covered by JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 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.

ESP Administrators will have access to the full range of administrative and system management information for the ESP system. In such situation, ESP administrators may have access to information collected from the tool and service applications. The purpose of access to this information is for 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 ESP Administrators because all Federal Government Agencies are required to implement email security within the agency.

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.

Each member of the JSOC security staff, Cybersecurity Services Staff, security analysts and engineers are granted role-based access to the ESP-Cloud console by the ESP-Cloud system administrator and in accordance with the DOJ's ESP-Cloud Account Management Procedures. The Account Management Procedures document and ESP-Cloud's access controls restrict email alert access only to security personnel that are responsible for and cleared to perform threat analysis.

Email users (DOJ or external Federal agency subscribers) may have access to view their individual spam digest within the platform. Users access their individual digest via a unique link provided to them, but users will not have ESP-Cloud system access.

Individuals are notified that the email records are maintained in ESP-Cloud that manages system services can be accessed or amended, in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (July 14, 2021), JUSTICE/JMD-026, *Security Monitoring and Analytics Service Records*, 86 Fed. Reg. 41089 (July 30, 2021) and JUSTICE/DOJ-003, *Correspondence Management System (CMS) for the Department of Justice,* 66 Fed. Reg. 29992 (June 4, 2001), 66 Fed. Reg. 34743 (June

29, 2001), 67 Fed. Reg. 65598 (October 25, 2002). However, DOJ has exempted these SORNs from access and amendment provisions of the Privacy Act.

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):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO completed 1/28/2025. Expires 1/28/26. **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:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The ESP-Cloud information system team has completed the system categorization in accordance with the service provided and information collected.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The ESP Cloud system has vulnerability and configuration scans completed monthly by the Cloud Service Provider (FireEye). The ISSO also performs continuous monitoring of the system through 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:** Audit logs are collected daily. By policy, all DOJ systems are subject to periodic audit, evaluation, and re-authorization for compliance with Federal and DOJ security and privacy standards.
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 information system information technology Rules of Behavior both prior to accessing the DOJ network, and annually thereafter. System administrators, including ESP-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 ESP-Cloud to include physical, logical access, identification, authentication, vulnerability management, auditing, and other assessment actions to ensure that security controls are operating as intended. The ESP-Cloud makes use of separate Privileged and Non-Privileged user accounts and leverages additional role-based access control technologies that allow for administrator session recording. All system log data are being sent to the centralized audit log management system for triage and review.

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.

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:

JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (July 14, 2021),

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

JUSTICE/DOJ-003, *Correspondence Management System (CMS) for the Department of Justice,* 66 Fed. Reg. 29992 (June 4, 2001), 66 Fed. Reg. 34743 (June 29, 2001), 67 Fed. Reg. 65598 (October 25, 2002).

Other published DOJ SORNs depending on the nature of information in the communication or collaboration document and how the information is retrieved.

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.***

The DOJ ESP Cloud may collect PII to include names, personal e-mail addresses, business e-mail addresses, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of actions, queries run, and contents of files). There are privacy risks such as potential unauthorized access to and disclosure of PII information through a system compromise. To mitigate these risks, information is stored in the ESP-Cloud system for only 30 days and ESP-Cloud records are managed in accordance with applicable federal records retention schedules. Also, ESP-Cloud information is only used by DOJ for the limited purpose of security investigation by JSOC security personnel and engineers, who have access on a need-to-know basis. To further mitigate risks associated with these activities, the ESP Cloud implements encryption, account management, access controls, auditing, and system monitoring tools to mitigate and protect privacy information.

To mitigate risk of unauthorized access to and disclosure of PII through a system compromise associated with emails, ESP Cloud uses encryption and logging controls for mitigation purposes. ESP Cloud 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.

By Department Order, all DOJ System Administrators with access to the information system 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 the IT systems, provides a review of the user's role in protection these systems, and established guidelines to follow at work and in mobile settings to protect against attacks on IT systems. Additionally, specialized security and privacy awareness training is required annually for privileged users and for managers.

All employees and contractors must also annually sign a 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.

To ensure the continued relevance, effectiveness of security controls, the ESP-Cloud system ISSO is responsible for the risk assessments, including privacy and security control assessments annually. In accordance with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.