United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Executive Correspondence Action Tracking Service (eCATs)

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)
U.S. Department of Justice

Date approved: [June 9, 2021]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (DOJ or "the Department"), Justice Management Division (JMD), Office of the Executive Secretariat (ExecSec) developed the Executive Correspondence Action Tracking Service (eCATs) tool to provide direct support to DOJ leadership by facilitating quality document management. eCATs is a commercial-of-the-shelf (COTS) software product that has been adapted to receive, process, and manage electronic correspondence for the Office of the Attorney General (AG), Office of the Deputy Attorney General (DAG), the Office of the Associate Attorney General (ASG), and other DOJ Component leadership. This product will assist Department leadership in facilitating and tracking written communications, including letters, information memos, action memos, and decision memos. This COTS product was procured through Procentix and Microsoft Dynamics.

JMD has prepared this Privacy Impact Assessment because eCATs will process, collect, maintain, use, and disseminate Personally Identifiable Information (PII). That is, eCATS is capable of processing PII that is not solicited but volunteered by members of the public who may be sending or receiving correspondence from the AG, DAG, ASG, and other Departmental Components, among other categories of information.

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.

In executing the responsibilities of the Department, DOJ leadership must draft, process, and sign executive-level correspondence and other written documents. eCATs will be utilized to automate the process of reviewing, analyzing, controlling, and tracking such executive-level correspondence and other written documents. These documents include correspondence received through DOJ's Mail Referral Unit, delivered directly to ExecSec via physical messenger, or sent to DOJ from the White House or Congress.

ExecSec is primarily responsible for controlling and managing executive-level correspondence for DOJ leadership, and will be primarily responsible for administering eCATS. In addition to ExecSec staff, some DOJ component users will access the system to submit prepared executive-level correspondence for action by DOJ leadership or act on executive-level correspondence before submission to appropriate DOJ leadership for signature or other final action. For instance, a DOJ component may be asked to first concur with a proposed DOJ leadership action before it is submitted to DOJ leadership for final approval. DOJ components with licenses, authorized for access by ExecSec, can log into eCATS to provide responses to executive-level correspondence either as .pdf or .docx documents.

eCATs is integrated with DOJ's identity management service, DOJ Identity and Access

Management (IamDOJ).[1] Access to data and the application is controlled by PIV user authentication and a detailed set of permissions, which correspond to the roles assigned to users by ExecSec. Users access the eCATS web application from their DOJ-issued workstation using a browser, such as Internet Explorer. User accounts are recertified on a yearly basis by the system administrator.

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

Authority		Citation/Reference
X	Statute	5 U.S.C. § 301 44 U.S.C. § 3101
	Executive Order	N/A
X	Federal Regulation	28 CFR § 0.77 (b)(e)
	Agreement, memorandum of understanding, or other documented arrangement	N/A
X	Other (summarize and provide copy of relevant portion)	Executive Correspondence Management Program Directive

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] IamDOJ is the official system of record for all DOJ identities. Within IamDOJ, each person is uniquely represented by an Enterprise Digital Identity (EDI), enabling governance, and reporting on identity attributes, permissions, and their associated system accounts. IamDOJ is covered by separate privacy compliance documentation.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	x	A, B, C, D	System users, correspondence or mail sent to the department, sender, recipient, and communication or mail sent to the department.
Date of birth or age	x	C, D	Information given by members of the public (US and non-USPERs)
Place of birth	x	C, D	Information given by members of the public (US and non-USPERs)
Gender	x	C, D	Information given by members of the public (US and non-USPERs)
Race, ethnicity or citizenship	x	C, D	Information given by members of the public (US and non-USPERs)
Religion	x	C, D	Information given by members of the public (US and non-USPERs)
Social Security Number (full, last 4 digits or otherwise truncated)	x	C, D	Information given by members of the public (US and non-USPERs)
Tax Identification Number (TIN)	x	C, D	Information given by members of the public (US and non-USPERs)
Driver's license	x	C, D	Information given by members of the public (US and non-USPERs)
Alien registration number	x	C, D	Information given by members of the public (US and non-USPERs)

(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
Passport number	x	C, D	Information given by members of the public (US and non-USPERs)
Mother's maiden name	x	C, D	Information given by members of the public (US and non-USPERs)
Vehicle identifiers			
Personal mailing address	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Personal e-mail address	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Personal phone number	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Medical records number	x	C, D	Information given by members of the public (US and non-USPERs)
Medical notes or other medical or health information	x	C, D	Information given by members of the public (US and non-USPERs)
Financial account information	x	C, D	Information given by members of the public (US and non-USPERs)
Applicant information	x	A, B, C, D	Information given by members of the public (US and non-USPERs) and federal employees.
Education records	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)

(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
Military status or other information	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Employment status, history, or similar information	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Employment performance ratings or other performance information, e.g., performance improvement plan	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Certificates	x	A, B, C, D	Federal employee resumes. Information given by members of the public (US and non-USPERs)
Legal documents	x	A, B, C, D	System users, correspondence or mail sent to the department, sender, recipient, and communication or mail sent to the department.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities	x	A, B, C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Criminal records information, e.g., criminal history, arrests, criminal charges	x	C, D	Information given by members of the public (US and non-USPERs)

(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
Juvenile criminal records information	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Civil law enforcement information, e.g., allegations of civil law violations	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Whistleblower, e.g., tip, complaint or referral	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Grand jury-related information	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Procurement/contracting records	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)

(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
Proprietary or business information	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	x	C, D	Correspondence communication or mail sent to the department. Information given by members of the public (US and non-USPERs)
- **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:			
- **User ID**	x	A	System users
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	x	A	System users
- **Queries run**	x	A	System users and Admin.
- **Content of files accessed/reviewed**	x	A	System users and Admin.
- **Contents of files**	x	A	System users and Admin.

(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,	Correspondence or mail received by DOJ may contain any PII provided by the sender of the correspondence or mail. Response letters may contain PII related to any matter that DOJ determines deserves correspondence or mail from DOJ, required or otherwise, authorized for disclosure.

3.2 Indicate below DOJ'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	x	Online	x
Phone		Email	x		
Other (specify): Some correspondence received online (https://www.justice.gov/doj/webform/your-message-department-justice) may require processing by DOJ leadership, at which point responses to the correspondence will be coordinated through eCATS.					

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): Correspondence could be referred to the Department from entities within and outside DOJ, including but not limited to Congress and the White House.					

Non-government sources:					
Members of the public	x	Public media, Internet		Private sector	x
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	JMD users can share documents, dashboards, and searches within the application.
DOJ Components			X	DOJ users can share documents, dashboards, and searches within the application.
Federal entities	X	X		Records Officers will share, or transfer, archived records to NARA. DOJ may share documents when responding to requests from Congress or the White House.
State, local, tribal gov't entities				
Public	X			DOJ users can share documents to answer public FOIA requests.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			DOJ users can share documents as part of litigation to courts or counsel during discovery.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise

privacy protected.

No information from eCATs will 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.

Two SORNS are applicable to eCATS. First, individuals have been notified that correspondence and action tracking records maintained in this system for the purpose of tracking correspondence received or originated by the Department or referred to the Department are covered by JUSTICE/DOJ-003, "Correspondence Management Systems (CMS) for the Department of Justice" last published at 66 Fed. Reg. 29992 (June 4, 2001); 66 Fed. Reg. 34743 (June 29, 2001); 67 Fed. Reg. 65598 (Oct. 25, 2002); 82 Fed. Reg. 24147 (May 25, 2017). Second, individuals have also been notified that account, audit log, and user records maintained in this system for the purpose of monitoring system activity and responding to cybersecurity incidents are covered by 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).

In addition, a Privacy Act Statement is provided when individuals submit information online at https://www.justice.gov/doj/webform/your-message-department-justice. It is not otherwise practical to provide individuals personalized notice on the collection, use, sharing, or processing of their PII when they voluntarily submit such information to the Department via physical mail or email. Public correspondences received by the White House or Members of Congress are forwarded to DOJ to provide responses. In compliance with the Privacy Act of 1974, Members of Congress should have the individuals who contact them sign privacy releases or waivers to acknowledge and consent to the Department disclosing records about the individuals to Members of Congress or their staff. Signed releases or waivers are generally included with correspondences forwarded from Members of Congress.

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.

Correspondence with Department leadership is generally not required. Individuals voluntarily send correspondence to DOJ for its response. Once submitted, the Department will use and/or disseminate correspondence, including PII submitted, in accordance with law and DOJ policy. Individuals will generally not be able to participate in how this

information will be used and/or disseminated. To the extent that the information is sent from another government source, e.g., a Congressional office, to DOJ, the individual may have consented to the release of their personal information. In any event, DOJ must respond to these inquiries, as appropriate.

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 correspondence and action tracking records maintained in this system for the purpose of tracking correspondence received or originated by the Department or referred to the Department can be accessed or amended in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-003, "Correspondence Management Systems (CMS) for the Department of Justice," last published at 66 Fed. Reg. 29992 (June 4, 2001); 66 Fed. Reg. 34743 (June 29, 2001); 67 Fed. Reg. 65598 (Oct. 25, 2002); 82 Fed. Reg. 24147 (May 25, 2017).

Individuals have also been notified that account, audit log, and user records maintained in this system for the purpose of monitoring system activity 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 DOJ 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:** *expected completion date is 05/28/2021* **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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** *User, groups, and document security were implemented in the system. Document version control is in place. Audit and activity logs are available for viewing.*
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:** *System logs are reviewed in accordance to OCIO policy and case by case security incidents.*
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:** *Cybersecurity Awareness 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?

eCATS has a security categorization of FISMA Moderate, and DOJ has implemented all applicable privacy and security controls for a Moderate baseline. In addition, users must complete the Department's Cybersecurity Awareness Training and sign the Department's Rules of Behavior General User Agreement before accessing eCATS. System administrators must also complete the Department's Cybersecurity Awareness Training; they, however, sign the Department's Rules of Behavior Privileged User Agreement to receive elevated permissions. The system administrator within ExecSec will monitor the eCATS accounts.

eCATS utilizes Secure Sockets Layer (SSL), which enables encrypted connection compliant with the Federal Information Processing Standard Publication (FIPS) 140-2.[2] eCATS is a Microsoft Dynamics Software-as-a-Service (SaaS) web application hosted in the Microsoft FedRAMP GCC High data center.[3] Sensitive information, including certain PII, are identified in documents by ExecSec Correspondence Analysts. They mark the electronic work package with a "Sensitive" flag and restrict users and group access to the

[2] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/publications/detail/fips/140/2/final.
[3] The FedRAMP program is a "government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services." Gov't Service Admin, FedRAMP, https://www.gsa.gov/technology/government-it-initiatives/fedramp (last visited May 6, 2021). More information on the FedRAMP program can be found at: https://www.fedramp.gov.

work package. They also have the option to redact sensitive information from document by using Adobe PDF Reader functions. The work package will display a "Sensitive" flag or notification banner to users with permission to view the record.

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.)

The information will be retained for 25 years and disposed of at the end of the retention period by electronic transmission to the National Archives and Records Administration (NARA). Once receipt is confirmed by NARA, the records are removed from the system. These records have been assigned record schedule number DAA-0060-2017-0002.

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-003, "Correspondence Management Systems (CMS) for the Department of Justice," last published at 66 Fed. Reg. 29992 (June 4, 2001); 66 Fed. Reg. 34743 (June 29, 2001); 67 Fed. Reg. 65598 (Oct. 25, 2002); 82 Fed. Reg. 24147 (May 25, 2017).

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 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to DOJ 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.***

Because users across DOJ will have access to eCATS, there are risks that: (1) unauthorized users will gain access to information, including PII in; (2) authorized users will gain unauthorized access to information, including PII; and (3) authorized users may mishandle information, including PII, maintained in this system. To mitigate these risks, eCATS users must complete the Department's Cybersecurity Awareness Training and sign the Department's Rules of Behavior General User Agreement before accessing the system. System administrators must also complete the Department's Cybersecurity Awareness Training; they, however, sign the Rules of Behavior Privileged User Agreement to receive elevated permissions. All eCATS users and system administrators will access, or authenticate into the system, using their PIV card. The ExecSec system administrators for eCATS are responsible for reviewing the system's login activity and notifying components to certify their assigned accounts to remain active. An account is disabled or removed from the system's access group when it is not used for more than 90 days.

eCATS has auditing controls that include tracking all actions taken by users, including when users access the system, when users update field values, and which users delete records. By compiling an audit trail or log of these actions, each user can be held accountable for each action they take. These audit controls mitigate the risk of malicious or inadvertent actions regarding work packages in eCATS.

Audit logs are also available to review when certain records are accessed in the system. When users conduct a search, the search results will display non-sensitive records unless the user has been given access to sensitive records. An audit of each user's search activity can be conducted.

Additionally, as the permanent records holder for DOJ's Senior Leadership Offices, ExecSec does not actively solicit dates of birth, SSN, or medical records. This information may be voluntarily provided by members of the public to DOJ via letters, emails, and fax. ExecSec maintains the records in accordance to the applicable records retention schedule. When PII or sensitive information are discovered, ExecSec follows these operating procedures to protect the data:

- When PII or sensitive information are identified in documents, the ExecSec Correspondence Analyst marks the electronic work package with a "Sensitive" flag, and a notification banner is displayed at the top of the work package for all viewers.
- The analyst then restricts users and group access to the work package, and the analyst has

the option to redact sensitive information from document by using Adobe PDF Reader functions.

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