Executive Office for U.S. Attorneys (EOUSA)

Privacy Impact Assessment
for the
USA Case Management Enterprise System (USACMES)

Issued by:

Kevin Krebs

Senior Component Official for Privacy

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 26, 2025

(May 2023 DOJ PIA Template)

Section 1: Executive Summary

The USA Case Management Enterprise System (USACMES) provides case management for the Executive Office for U.S. Attorneys' (EOUSA) and the 94 U.S. Attorney's Offices (USAOs) nationwide. USACMES is an environment which includes, but is not limited to, applications related to case management, resource tracking, grand jury tracking, security incident reporting, and other administrative tracking systems. USACMES is managed by the Enterprise Application Development (EAD) in EOUSA, who develop and deploy applications within USACMES.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

EAD acquires or develops, then deploys a variety of applications to support EOUSA and the USAOs. USACMES is a management information system (MIS) that includes applications used by attorneys and litigation support staff to track details and content relevant to criminal and civil investigations and federal court cases throughout the lifecycle of the litigation. Statistics from the system may also be used to measure AUSA workload productivity.

CaseView Case Management System
CaseView is the case management system (CMS) application supporting all USAO districts. CaseView is designed to track and manage individual case information from initiation through final disposition. CaseView provides a graphical interface into the Legal Information Office Network System (LIONS) database. Functions include:

- Civil Docketing
- Criminal Docketing
- Document Repository and PACER Link
- Manuals and Policies
- Records Center
- Reporting and Management

Grand Jury Tracking System (GJTS)
The objective of the GJTS is to automate the various Grand Jury workflow and document generation processes performed by USAO personnel. The GJTS will enable users to perform all Grand Jury functions from a single web-based application accessed through USAO Applications Portal. The GJTS functionality includes:

- Search and track Grand Jury Cases and Subpoenas.
- Support multiple Grand Jury matters within a USAO district.

- Upload local Grand Jury Subpoena attachments.
- Schedule Grand Jury time slots via electronic calendar.
- Forward scheduled Grand Jury time slot to AUSA Outlook calendar.
- Searchable database of vendors that are used to support cases, including contact information and Taxpayer Identification Number.
- Searchable Agent database including 6(e) Form to comply with Federal Rule of Criminal Procedure.
- Searchable Law Enforcement Agency database of those agencies involved in cases.
- Automated Forms (Grand Jury Subpoena, USA-211, USA 212, Litigation Expense, OBD-2, DOJ-3, and Fax Transmittal).
- Reporting.

Consolidated District Information System (CDIS)
The Consolidated District Information System (CDIS) is a secure Web-based system used to manage the official titles, collateral duty assignments, and emergency contact information for personnel in the U.S. Attorney community. The system manages emergency contact information for all employees and contractors in the U.S. Attorney community. The information contained in CDIS is critical to the ability of the Executive Office for United States Attorneys (EOUSA) to locate and contact key personnel in the districts, particularly during emergencies and other urgent situations.

The primary purpose of CDIS is to provide every employee and contractor a mechanism for entering and maintain their own telephone numbers and emergency points of contact in CDIS. The contact information in CDIS feeds the enterprise-wide Employee Notification System (ENS). The ENS will quickly notify USAO and EOUSA employees and contractors when unexpected events or emergency situations impact the workplace. The ENS transmits alert messages via conventional and mobile telephones, pagers, electronic mail, and Short Message Service (SMS) text. The contact information is used for preparation of general phone and mail lists, as well as for emergency contact and emergency notification listings.

United States Attorneys' Resource Summary Reporting System (USA-5)
The United States Attorneys' Resource Summary Reporting System (USA-5) is a time tracking application used to manage and analyze personnel resources allocated (by program category) to the United States Attorneys' Offices (USAOs). USAO staff enter and submit their category allocation information on a weekly basis. Visibility of information entered within the application is delegated through rule-based access controls, facilitated by administrators or authorizing officials (AO).

USA Grants
USA Grants is a web-based system facilitating the distribution of grant solicitations and the feedback for pending applications between DOJ's Office of Justice Programs (OJP) and EOUSA/USAOs. The system also facilitates the distribution of pre-award notifications for soon to be awarded grants. The system will alert users by email and dashboards when new grant solicitations, pending applications, and pre-award notifications are received from OJP and ready for review. The system also assists with management reporting showing pending applications reviewed and feedback provided by each office.

United States Attorneys Incident Reporting System (USA-R)
Security incident reporting in USACMES is done with the USA-R (United States Attorneys Incident Reporting System) application, which is utilized by employees. USA-R is a web-based system used for processing security incidents, urgent threats, system security incidents, case-related urgent threats, and emergency incidents. The system also allows authorized users, (specifically those users authorized to use the system by a system manager or AO; where rule-based access controls (RBAC) are delegated through the USAauth/Okta Identity Management System[1]), to route, track and report on the information contained in the system.

PACER Management and Billing System (PMBS)
The Public Access to Court Electronic Records (PACER) service provides electronic access to federal court records. PACER provides registered users with instantaneous access to documents filed at all federal courts. The PACER Management and Billing System (PMBS) supports PACER users at EOUSA and all USAO districts in managing the PACER invoice process by automating the management, distribution, and verification of PACER invoices by each district's designated Legal Resource Manager (LRM).

Transit Subsidy Management and Billing System (TMBS)
Currently EOUSA offers a transit subsidy to qualifying employees through the Justice Employee Transit Savings (JETS) Program. The Resource Management and Planning (RMP) staff is responsible for the implementation and oversight of the JETS Program at EOUSA. Every month RMP receives a monthly activity report from DOT. TMBS automates the process of distributing the activity report to the 94 USAOs for review. Each USAO Transit Coordinator has the ability to provide feedback on any issues with their activity report to the JETS Program Coordinator for an appropriate resolution. Only those districts that have employees using a public transit system will use TMBS. TMBS is a component of USAInvoice.

Victim Services Tracking System (VSTS)
The Victim Services Tracking System (VSTS) is a data collection system that generates monthly, quarterly, and annual reports of USAO victim services data. VSTS is implemented by EOUSA to improve the accuracy, consistency, and frequency of the reporting of victim services to the Office for Victims of Crime (OVC). The system allows for uniform standards in reporting victim services statistics. VSTS provides district users the ability to track victim services provided, document training activities, and submit district-level Monthly Reports. In addition, Office of Legal and Victim Programs (OLVP) management staff can access summary Status Reports of data entered by all districts.

Gilglio
Giglio is another EAD-developed application within USACMES. The *Giglio* Management System is designed to equip prosecutors to fulfill their obligations under the United States Constitution, *Giglio v. United States*, 405 U.S. 150 (1972), and professional ethics rules. The

[1] USAauth is EOUSA's instance of Okta, a cloud-based Identity Provider (IdP), which is integrated with USAidgov, an Identity Management System (IDMS), to provide rule-based access controls to applications (e.g. general vs privileged users). Logging, access controls, and delegations within the IDMS ensure non-repudiation of any action(s) performed inside USACMES applications.

Department of Justice's *Giglio* Policy (Justice Manual 9-5.100) describes the mechanisms by which federal prosecutors gather potential impeachment information from DOJ investigative agencies and agency employees. All federal investigative agencies and their oversight agencies honor *Giglio* requests relating to law enforcement agency employees who may serve as witnesses or affiants in federal investigations and prosecutions. The *Giglio* Management System equips each USAO to more efficiently and accurately: (1) generate and track *Giglio* requests to law enforcement agencies, including oversight agencies such as the Office of Inspector General and Office of Professional Responsibility; (2) track and store information provided by the law enforcement agency and witness in response to *Giglio* requests as well as related documents/pleadings, to the extent permitted by JM 9-5.100 and Justice/DOJ–017 DOJ *Giglio* Information Files, 80 Fed. Reg. 16025-01 (Privacy Act System of Records); (3) categorize the type of information provided by the law enforcement agency; (4) track the manner in which the district handled the impeachment information for consistency in other matters; (5) search the system; (6) generate reports; and (7) ensure that *Giglio* After-Action reports are provided to federal agencies as required by JM 9-5.100 ¶ 8. Using Okta system information, each district will identify (1) *Giglio* Users, such as AUSAs, paralegals, and support staff, who are authorized to submit *Giglio* requests using the system; and (2) administrative personnel with *Giglio* request support duties and attorneys who are *Giglio* Requesting Officials who will manage the day-to-day flow of information in the system and have full access to that district's information. Each district's information will be limited to that district and will not be accessible to any other district.

Thomson Reuters ProLaw
The EOUSA General Counsel's Office (GCO) utilizes ProLaw, a commercial off-the-shelf software by Thomson Reuters. ProLaw, "combines case and matter management with time entry, billing, and accounting in one integrated solution." GCO uses ProLaw to manage general performance and disciplinary information, as well as performance improvement plans, warnings, and reprimands for government employees.

Developed applications like many of those described above are built upon a collection of Java specifications and APIs, then deployed into the Red Hat OpenShift Container Platform execution environment. OpenShift provides a large-scale, distributed, and high-availability infrastructure for the applications. Developed applications within USACMES are: CaseView, CaseView Admin, CDCS, CDIS, CDIS Sync, ReportGenerator, DMS, EAR-DAPS, Giglio, GJTS, GJTS Sync, LIONSNICS, NPDB, PMBS, PMBS Notification, Solrindex, TMBS, TMBS Notification, USA-5, USA-5 Summary Job, USA-5 Sync, USA-Grants, USA-R, USA-R Reminder Jobs, and VSTS.

Acquired applications, referred to as "commercial-of-the-shelf" (COTS) software, have several principal uses within the USACMES MIS. For example, SAP Crystal Reports is used to write meaningful reports from the structured data collected by USACMES applications, which is stored in relational databases and the USACMES Datawarehouse. SAP BusinessObjects is used to schedule delivery of these reports, providing stakeholders with meaningful information for mission critical decision making.

All applications within USACMES, both those developed in house and purchased commercially off the shelf, are standardized with features like transaction management,

security, web services, and connectivity to each of their respective databases. The USACMES environment is within the DOJ firewall, where application data is stored within Microsoft SQL Server databases that are encrypted, in compliance with data-at-rest IT Security policy.

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	28 U.S.C. §§ 516 and 547
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	JM 9-5.100 ¶ 8, 405 U.S. 150 (1972) OMB Exhibit 300, Capital Asset Plan and Business Case Summary

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Specific information types collected include: full name of system users and members of the public who are the subject of or otherwise identified in the underlying case
Date of birth or age	X	A, B, C, D	Specific information types collected include: date of birth of system users and members of the public who are the subject of or otherwise identified in the underlying case
Place of birth	X	A, B, C, D	Specific information types collected include: place of birth of system users and members of the public who are the subject of or otherwise identified in the underlying case
Sex	X	A, B, C, D	Specific information types collected include: sex of system users and members of the public who are the subject of or otherwise identified in the underlying case
Race, ethnicity, or citizenship	X	A, B, C, D	Specific information types collected include: race, ethnicity, or citizenship of system users and members of the public who are the subject of or otherwise identified in the underlying case
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B	Specific information types collected include: social security number (last 4 digits) of system users and members of the public who are the subject of or otherwise identified in the underlying case
Tax Identification Number (TIN)	X	A, B	Specific information types collected include: IRS EIN/TIN of system users and members of the public who are the subject of or otherwise identified in the underlying case
Driver's license			
Alien registration number	X	A, B, C, D	Specific information types collected include: alien registration number members of the public who are the subject of or otherwise identified in the underlying case
Passport number			
Mother's maiden name			
Vehicle identifiers			

(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
Personal mailing address			Specific information types collected include: home address system users and of members of the public who are the subject of or otherwise identified in the underlying case
Personal e-mail address	X	A, B	Specific information types collected include: personal email address of employees, used for emergency contact: Consolidated District Information System (CDIS) application
Personal phone number	X	A, B	Specific information types collected include: personal phone number of employees, used for emergency contact: Consolidated District Information System (CDIS) application
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	X	A, B	Specific information types collected include: internal complaints and communication between General Counsel's Office (GCO) staff, used only in ProLaw by Reuters, hosted within the system. Only GCO staff has access to the information through rule-based access controls
Certificates			
Legal documents	X	A, B	Specific information types collected include: Federal Rule of Criminal Procedure form 6(e), signed by agent(s) of government agencies; grand jury subpoena attachments; *Giglio* requests and related documents
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	A, B	System users may encounter URLs referenced in case data, e.g. PACER documents, public court filings
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	X	A, B, C, D	Specific information types collected include: metadata of criminal history, arrests, criminal charges of system users and members of the public who are the subject of or otherwise identified in the underlying case
Juvenile criminal records information	X	A, B, C, D	Specific information types collected include: Juvenile criminal records metadata of system users and members of the public who are the subject of or otherwise identified in the underlying case
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	Specific information types collected include: Civil law enforcement metadata, e.g., case numbers related to individuals who are the subject members of the public who are the subject of or otherwise identified in the underlying case
Whistleblower, e.g., tip, complaint, or referral	X	A, B	Information of this type is stored only in ProLaw, which is used only by the General Counsel's Office (GCO)
Grand jury information	X	A, B, C, D	Specific information types collected include: Grand jury metadata, e.g. Federal Rule of Criminal Procedure, form 6(e), related to agents and members of the public who are the subject of or otherwise identified in the underlying case
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	Specific information types collected include: witness contact information for individuals who are the subject of or otherwise identified to be a witness in the underlying case
Procurement/contracting records	X	A, B	Specific information types collected include: Procurement/contracting records of vendors working on cases, and the system or its application(s)
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B	Specific information types collected include: plotted points on maps for hospice locations (fentanyl research), district office locations and boundaries
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B	User IDs will appear in audit data generated by the system and forwarded into the Enterprise Security information and event management (SIEM) [Splunk] in compliance with executive order M-21-31
- **User passwords/codes**			Passwords are not used on the system; applications are integrated with USAauth (Okta) and USAidgov Identity Management System (IDMS) for single sign-on (SSO)
- **IP address**	X	A, B	IP addresses will appear in audit data generated by the system and forwarded into the Enterprise Security information and event management (SIEM) [Splunk] in compliance with executive order M-21-31
- **Date/time of access**	X	A, B	Date/time of access will appear in audit data generated by the system and forwarded into the Enterprise Security information and event management (SIEM) [Splunk] in compliance with executive order M-21-31
- **Queries run**	X	A, B	Information on when and who run database queries will appear in audit data generated by the system and forwarded into the Enterprise Security information and event management (SIEM) [Splunk] in compliance with executive order M-21-31
- **Contents of files**			

(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	Information pertaining to witnesses, confidential informants, and expert witnesses, as well as information pertaining to federal employees from other agencies that may be involved in litigation may be included. Other PII present in case files may also be included. Any other PII pertaining to reported security incidents or breaches may also be included.

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

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

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)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
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			Information is accessible only for those working on the case(s), through request via rule-based access controls. No application within the system is public facing on the Internet.
DOJ Components	X			Information is accessible only for those working on the case(s), through request via rule-based access controls. No application within the system is public facing on the Internet.
Federal entities	X			Information is accessible only for those working on the case(s), through request via rule-based access controls. No application within the system is public facing on the Internet.
State, local, tribal gov't entities	X			USAO case metadata maintained on the system (e.g. case numbers, time spent on case) is accessible only to those working on the case(s), through request via rule-based access controls; no evidence that can affect the outcome of the case(s) is stored. No application within the system is public facing on the Internet.
Public	X			Information is only shared with members of the public if vetted through the Privacy Act and the Freedom of Information Act (FOIA) processes. No application within the system is public facing on the Internet.

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 may be shared with opposing counsel, the parties to the litigation, and individuals in support of the litigation, such as experts and witnesses, along with the courts, as required. No application within the system is public facing on the Internet.
Private sector		X		Private companies under contract with USAOs to perform litigation support work. No application within the system is public facing on the Internet.
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 will not 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

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 Federal Register System of Records Notice (SORN) is provided to inform the public about the collection, use, sharing or other processing of PII data within the system. *See* USA-001, USA-003, USA-005, and USA-007. https://www.justice.gov/opcl/doj-systems-records#USA

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.

Individuals may decline to provide information requested directly from the individual. However, depending on the situation, failure to provide the information may for example result in access being denied to users of the system. Generally, individuals who are the subject of a law enforcement investigation do not have the ability to participate in the collection and dissemination of information as the information is in support of ongoing law enforcement activities.

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 can request data through the Privacy Act and the Freedom of Information Act (FOIA) processes. However, information may be withheld where the information is law enforcement sensitive or where disclosure would jeopardize ongoing law enforcement activities.

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):** ATO issued 7/24/2024. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** Currently, there are no open POA&Ms related to privacy.
	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:** System is continuously assessed using NIST 800-53 controls, which include an evaluation for all security objectives

	specified under FIPS 199; confidentiality, integrity, and availability. System has been designated as moderate by definition: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Security controls (NIST 800-53) are reassessed annually as part of Assessment and Authorization (A&A)
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 data generated by the system is forwarded into the Enterprise Security information and event management (SIEM) [Splunk] to comply with executive order M-21-31; logs are reviewed weekly
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**. Contractors who work on the system are subject to the following rules and policies: DOJ-02, Contractor Privacy Requirements clause DOJ-05, Security of Department Information and Systems clause FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems FAR 52.203-13 Contractor Code of Business Ethics and Conduct FAR 52.204-9 Personal Identity Verification of Contractor Personnel Contract Vehicles used: GSA 8(a) STARS III, GSA Alliant 2
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:** In addition to annual privacy and cybersecurity training, users complete Records and Information Management (RIM) Refresher Training, available and assigned in learnDOJ, is required by users of the system, annually.

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?

NIST 800-53 rev 5 Risk Management Framework controls are in place and assessed annually: Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Assessment, Authorization and Monitoring (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environmental Protection (PE), Planning (PL), Program Management (PM), Personnel Security (PS), PII Processing and Transparency (PT), Risk Assessment (RA), System and Services Acquisition (SA), System and

Communications Protection (SC), System and Information Integrity (SI), and Supply Chain Risk Management (SR). In addition, weekly review of audit logs, which include system logins and activity, are used to detect possible unauthorized access.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

To the extent any documentation generated within the system constitutes a "federal record," it is subject to the corresponding General Records Schedule or SF-115 Records Disposition Schedule governing such records. For a listing of existing case file records retention schedules approved by the Archivist of the United States, see USAM 3-13.310.

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-017, Giglio Information Files, 80 FR 16025 (March 26, 2015), available at: https://www.govinfo.gov/content/pkg/FR-2015-03-26/pdf/2015-06934.pdf.
Justice/USA-003, Citizen Compliant Files, 54 FR 42088 (Oct.13, 1989), available at: https://www.justice.gov/opcl/docs/54fr42088.pdf.
Justice/USA-001, Administrative File, 48 FR 56662 (Dec. 22, 1983), available at: https://www.justice.gov/opcl/docs/48fr56662.pdf.
Justice/USA-005, Civil Case Files, 53 FR 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf.
Justice/USA-007, Criminal Case Files, 53 FR 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf.
Justice/DOJ-002, DOJ Computer Systems Activity & Access Records, 64 FR 73585 (Dec. 30, 1999), available at: https://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf.

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?

Specific information being collected and data minimization strategies
Data contained within the system includes administrative metadata of cases, internal complaints and communication between General Counsel's Office (GCO) staff, and Federal Rule of Criminal Procedure 6(e) form signed by agents involved in the case(s). Risk of exposure would introduce issues of data integrity, personnel safety, and could affect the outcome of pending litigation. This risk is mitigated through limiting access of the information to individuals who have a need-to-know, working on the case(s). Data is also controlled internally through rule-based access controls (RBAC). See 4.1 for specified data types. The system is also within the DOJ firewall, where application data is stored within Microsoft SQL Server databases that are encrypted, in compliance with data-at-rest IT Security policy.

Sources of the information
The information stored on the system is provided by the United States Attorney's Offices, who obtained the information in the course of civil and criminal investigations and litigation. Underlying case information is obtained from individuals involved in the cases, including law enforcement organizations, federal employees and contractors. To the extent possible, the information in the system is limited to metadata and only that information needed from a criminal or civil case file to perform the functions necessary in the system is entered into the USACMES.

Specific uses or sharing
The USACMES is strictly limited to EOUSA and USAO personnel to execute their official functions. The applications are narrowly-tailored and specific to the execution of investigations and the prosecution of federal cases. For example, some of the applications are strictly for administrative uses, such as case tracking, resource allocation, time management. Whereas other applications include the execution of specific aspects of a litigation, such as the GJTS and *Giglio* applications. Information used in each application is unique to the application and its function, and is limited to that particular application accordingly. For example, information in the *Giglio* application is not shared across any other applications. Similarly, information in each application is only shared with authorized individuals on a need-to-know basis in conformity with the law and policy. Access to the system is strictly controlled through rule-based access controls, facilitated by administrators or AOs.

Privacy notices to individuals
Generally, individuals who are the subject of a law enforcement investigation do not receive Privacy Act notices when information is collected in the course of an investigation or prosecution. Rather, this PIA and the applicable SORNs identified herein serve as notice to the public that information about individuals subject to or otherwise involved in investigations or litigation may be used and maintained in this system, and the SORN details the use, maintenance, and disposition of information in the system of records.

Decisions concerning security and privacy administrative, technical, and physical controls over the information.
Rule-based access controls are enforced by authorizing officials and administrators who maintain the system. As described above, access is granted to certain applications by District System Managers through USAauth (Okta) and the USAidgov Identity Management System (IDMS). Authorizations are reviewed through annual account recertification. The system is comprised of virtual servers, which are physically hosted at the Network Operations Center (NOC) in Columbia, South Carolina, USA. Any connected system (sources of data) that contains cloud components follows the FedRAMP Moderate

Authorization baseline. Audit logs are reviewed weekly, and privacy and security controls are reassessed annually. Users are provided with onboarding and annual security and privacy training, and have to acknowledge and sign Rules of Behavior before they are granted access to the system.