

Criminal Division



Privacy Impact Assessment for the Capital Case Database

Issued by:
Jennifer A.H. Hodge
Criminal Division, Senior Component Official for Privacy

Approved by: Andrew J. McFarland
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: February 10, 2026

(October 2023 DOJ PLA Template)

Section 1: Executive Summary

Capital punishment is an essential tool for deterring and punishing those who would commit the most heinous crimes and acts of lethal violence against American citizens. The United States Department of Justice (Department or DOJ), Criminal Division (Division), Capital Case Section (CCS) functions to ensure appropriate application of the death penalty throughout all federal jurisdictions. Each decision must be based upon the facts and law applicable to the case as well as the [Executive Order](#) guiding the principles of its application.

The CCS manages this process and facilitates the Attorney General's Review Committee on Capital Cases (AGRCCC or Committee)¹ in its evaluation of capital cases submitted by United States Attorneys (USAs) or Assistant Attorney Generals (AAGs) to the Department for review and recommendation to the Attorney General (AG). The CCS conducts a preliminary analysis of all cases in which the USA or AAG may or must charge a defendant with a crime punishable by death and advises the AGRCCC of the factual and legal issues that are relevant to the Committee's decisions. In appropriate cases, the AGRCCC will make recommendations to the AG, who ultimately decides whether to authorize a capital prosecution. CCS manages this process using the Capital Case Database (CCD). CCD serves as the master file and case management system for the Department's capital cases.

The Division conducted this Privacy Impact Assessment (PIA) to assess and mitigate the risks to the personally identifiable information (PII) collected in this system, which includes but is not limited to substantial identifying, situational and psychological information about the defendant, their alleged crime and slightly more limited information about the victim(s).

Section 2: Purpose and Use of the Information Technology

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

The capital case review process administered by CCS culminates in a decision to seek, or not to seek, the death penalty against an individual defendant. Each such decision must be based upon the facts and law applicable to the case and be set within a framework of consistent and even-handed national application of Federal capital sentencing laws. Fairness requires all reviewers to evaluate each case on its own merits and on its own terms. The overriding goal of the review process is to allow proper individualized consideration of the appropriate factors relevant to each case. Reviewers must take care to contextualize a given case within national norms and historical practice. For this reason, the multi-tier process used to make capital

¹ The AGRCCC is composed of attorneys from the Office of the Deputy Attorney General and the Office of the Assistant Attorney General for the Criminal Division (AAG CRM), and at-large prosecutors from the United States Attorneys' Offices and other Department components. The AAG CRM may fill at-large Committee member positions with prosecutors who will serve for renewable, limited terms of two years.

prosecution authorization decisions is designed to provide reviewers with access to the national decision-making context and, thereby, to reduce disparities across districts.

As with all other actions taken in the course of Federal prosecutions, arbitrary or impermissible factors—such as bias for or against an individual based upon characteristics such as race, ethnicity, or religion—will not inform any stage of the decision-making process. In order to assure the most impartial decision possible, the Department employs a multi-layered review process which ultimately relies on the AG to ensure that politics, personal principles, and local norms are removed from the process.

The vast majority of death eligible cases originate from the Judicial Districts which are under the purview of the USAOs. A few cases may originate from the various investigative Divisions within the Department, which fall under the purview of the Division's AAG. Within the originating office the format of the reviewing body is at the discretion of the USA or the AAG, however the relevant factors and analysis are guided by the uniform and leveling framework mandated within the Justice Manual (JM)² and in mandatory consultation with CCS. CCS provides experiential expertise and extensive reference materials to prosecutors of capital-eligible cases on their intranet site, known as DOJNet,³ which is available to Department employees. The USA or AAG will present their detailed recommendation along with mandatory factual and analytical information to CCS, who initiates the next layer of review.

Absent extenuating circumstances, prior to seeking an indictment charging a capital-eligible offense, the USA or AAG shall submit the case to CCS for review.⁴ In instances in which the government cannot legally pursue the death penalty due to the inability to prove an eligibility factor, the prosecution's reliance on the defendant's proffer protected statements for proof culpability, or the need to extradite the defendant from a country that requires assurances against the employment of capital punishment, the USA or AAG can request an expedited decision with a streamlined submission process.⁵ In all other circumstances,⁶ the submission package aims to create a detailed picture of all elements surrounding the crime(s) in question, the defendant, the victim(s) and any mitigating or aggravating circumstances which may aid in rendering the most rigorous evaluation possible.

Upon receipt of the submission package, CCS manages the remainder of the evaluation process using the CCD. Additionally, an electronic working file is created in an access-controlled⁷ folder on the Division's share⁸ drive. CCS will enter the submission package into CCD to

² <https://www.justice.gov/jm/jm-9-10000-capital-crimes>.

³ DOJNet is an intranet site accessible to Department employees only and managed by the Department. DOJNet contains prosecutorial, administrative, security, personnel and human resource reference materials, policies, procedures, directives, announcements and other job-related professional materials.

⁴ Procedures for exigent circumstances, and the ultimate requirement to submit a capital eligible case for review a minimum of ninety (90) days prior to the court's deadline to file a notice of intent to seek a the death penalty are described in [JM 9-10.060 - Mandatory Pre-Indictment Review](#).

⁵ [9-10.070 - Expedited Decision Submissions](#).

⁶ A full description of the required submission package is located at [JM 9-10.080](#).

⁷ The access level is determined based on the minimum access necessary to complete necessary duties. Members of the AGRCCC are not permitted access.

⁸ The Division share drives are part of the Division's JCON infrastructure support. An IPA is presently under development for this system. Share drives have access controls which compartmentalize a user's access to their Section and then imposes further access controls specific to the needs of the Unit, project or user group based on their need-to-know.

initiate the creation of the case file. The information contained in the submission package and specifically defined in the JM⁹ includes;

- A prosecution memo containing:
 - Pertinent deadlines;
 - A narrative on the facts of the case and the supporting evidence;
 - Relevant prosecutorial considerations;
 - A discussion of the federal interest in bringing federal charges and capital charges, including a discussion of the standards for determination set forth in 9-10.140 - Standards for Determination;
 - Background and criminal records of the capital eligible defendants;
 - Background and criminal record of the victim;
 - Victim impact information from the family or other victim impact evidence;¹⁰
 - Foreign citizenship information as it relates to the Vienna Convention on Consular Relations;¹¹ and
 - Recommendation of the USA or AAG.
- Death Penalty Evaluation Form relevant to the specific offense;¹²
- Non-Decisional Information Form (discussed further below);
- All existing and proposed indictments and superseding indictments;
- Draft notice of intent to seek the death penalty that would be filed with the court (only if the USA or AAG recommends seeking the death penalty);
- Materials provided by the defense counsel;¹³
- Point of contact (assigned attorney); and
- Relevant court decisions.

When the submission package is perfected, CCS circulates it to the AGRCC, which may convene meetings on its own or with counsel for the parties. The AGRCC consists of one member each from the Office of the Deputy Attorney General (DAG) and the Office of the AAG for the Criminal Division (AAG CRM), and at-large prosecutors from the United States Attorneys' Offices and other Department components. Members of the committee will review the matter, seek necessary input from the prosecutor and defense attorney, perform their own legal analysis and discussion of the case, and then through a voting process they render a recommendation to the AG.

CCS authors a memo which incorporates the AGRCC's recommendation to the AG, who will document the decision in a letter to the prosecuting office. The appropriate USAO or AAG is advised of the decision in order to proceed in accordance. Should there be requests to

⁹ See supra at note 8.

¹⁰ Absent extenuating circumstances the USA/AAG will consult with the family of the victim to determine their wishes in addition to advising them of their rights pursuant to 18 U.S.C. § 3771.

¹¹ See JM 9-2.173 and Fed. R. Crim. Pro. 5(d)(1)(F).

¹² Death Penalty Evaluation Forms are offense-specific and include [homicide](#), [narcotics](#), and [espionage/treason](#). Death Penalty Evaluation forms are "check box" forms to affirmatively identify the factors defined in 9-10.140 - Standards for Determination that the prosecutor believes meet the minimum standard of proof.

¹³ No final decision to seek the death penalty shall be made if defense counsel has not been afforded an opportunity to present evidence and argument in mitigation.

amend a decision to seek the death penalty by either the prosecuting office or the defendant, they must be justified in writing and pass through another review by the ARGCCC and then the AG. As the case passes through the decisional process, updates in the status, committee member opinions, relevant review factors and the analytical, recommendation and decisional memos are added to CCD. Key case personnel who submitted the package are recorded for contact purposes. Personnel involved in all aspects of the analysis and decision process are documented and the decisions are recorded. Additionally, CCD will issue automated reminders to the CCS staff when updates on cases that met the exigent circumstances criteria for seeking an indictment prior to the review process are due.

Access to CCD is limited to CCS personnel and tiered based on their need-to-know. The CCS Administrative Team has full access to the database to allow the entry and maintenance of data. CCS managers and case attorneys have modified full access to the database, and the ability to view uploaded documents and data related to their case analysis, but no access to certain demographic data (see discussion of the Non-Decisional Information Form below). There is no outside access to this system. Members of the ARGCCC do not have access to CCD but are provided the relevant decisional documents on a case-by-case basis via email. Also, on a case-by-case basis the AGs decisions are shared with the prosecuting office. Much of the information within CCD is held within the strictest confidence.¹⁴ The decision-making process preliminary to the Department's final decision is confidential. Information concerning the deliberative process may only be disclosed within the Department and its investigative agencies as necessary to assist the review and decision-making process. Likewise, the information is not subject to discovery by the defendant or the defendant's attorney.¹⁵ These information practices restrict the flow of information to the submitting office as the appropriate gatekeeper.

The historical scrutiny of the death penalty and its application have led to numerous audits, studies and Departmental directives¹⁶ identifying the need to collect demographic information on both the defendant and victim(s) in order to assess its fair application and "maintain public confidence in the fairness of the process by making more complete racial and ethnic data available for both actual and potential federal capital cases on a continuing basis."¹⁷ However, that self-same demographic information must be withheld from the CCS attorneys working on the case analysis, the members of the ARGCCC and the AG because it is not relevant to the decision and the mere knowledge of the information could be considered a potential introduction to possible bias into the process. Thus, in order to wall-off demographic information from those in the decisional process, the reporting of demographic information is isolated to a specific form called the Non-Decisional Information Form. The Non-Decisional Information Form is designed as a mechanism to control and limit access to demographic information to those CCS employees with a specific need-to-know but no role in the decision.

¹⁴ <https://www.justice.gov/jm/jm-9-10000-capital-crimes#9-10.050>.

¹⁵ [Fed. R. Crim. P. 16\(a\)\(2\)](#).

¹⁶ The most prominent of these are the [RAND Corporation Study "Race and the Decision to Seek the Death Penalty in Federal Cases," 2006](#) and [U.S. DOJ Report "The Federal Death Penalty System: Supplementary Data, Analysis and Revised Protocols for Capital Case Review," June 6, 2001](#). This 2001 Report first directed that "U.S. Attorneys will be required to submit information, including racial and ethnic data, about potential capital cases, as well as those in which a capital offense is actually being charged."

¹⁷ *See id.*, 2001 U.S. DOJ Report.

The submitted form itself is not uploaded into the database, but stored in an access-restricted folder in the CCS share drive. The demographic information within the form, is entered into the database in access-restricted fields, which cannot be viewed by those in the decisional process but can be accessed by the CCS Administrative team for purposes of generating the statistical information needed for audits or studies of the decisional process.

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	5 U.S.C. § 301; 18 U.S.C. §§ 3591 to 3599; 28 U.S.C. §§ 510, 516, 519
☒ Executive Order	Restoring the Death Penalty and Protecting Public Safety, January 20, 2025
☒ Federal Regulation	28 C.F.R. § 0.55
☐ Memorandum of Understanding/agreement	
☒ Justice Manual ¹⁸	Justice Manual: Title 9, Criminal; 9-10.000
☐ Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

¹⁸ <https://www.justice.gov/jm/justice-manual>.

(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
<i>Example: Personal email address</i>	X	B, C and D	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	X	A, B, C & D	Names of defendants, victims, government personnel involved in all aspects of the decision process are contained in CCD. Names of defense attorneys, victim family members, witnesses or other individuals may appear in narrative information. *
Date of birth or age	X	C & D	Defendant and victim DOB are recorded in CCD. This information may appear in narrative information for the defendant or victim if it is relevant to the decision.
Place of birth	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Sex	X	C & D	Defendant and victim sex are recorded in CCD. This information may appear in narrative information for the defendant or victim.
Race, ethnicity, or citizenship	X	C & D	Defendant and victim race and ethnicity are recorded in CCD. Race, ethnicity, and citizenship information is captured as demographic information for the defendant or victim in the Non-decisional Information form.
Religion	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Driver's license	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Alien registration number	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Passport number	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Mother's maiden name	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.

(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 Detainees; 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	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Personal mailing address	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Personal e-mail address	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Personal phone number	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Professional mailing address	X	A, C, & D	Prosecutorial professional contact information is captured in CCD. The defense counsel may provide this information in the narrative information.
Professional e-mail address	X	A, C, & D	Prosecutorial professional contact information is captured in CCD. The defense counsel may provide this information in the narrative information.
Professional phone number	X	A, C, & D	Prosecutorial professional contact information is captured in CCD. The defense counsel may provide this information in the narrative information.
Social Media Identifiers	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Medical records number	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Medical notes or other medical or health information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Financial account information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Applicant information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Education records	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Military status or other information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.

(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 Detailers; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Employment status, history, or similar information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Certificates	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Legal documents	X	C & D	Existing and draft indictments and the draft Notice of Intent to seek the Death Penalty will be included in the submission package where seeking the death penalty is proposed. Additional legal documents related to relevant offenses may be included if relevant to the decision.
Device identifiers, e.g., mobile devices	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Web uniform resource locator(s)	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Foreign activities	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Criminal records information is recorded in CCD for the defendant and victim. This may appear in narrative information. This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Juvenile criminal records information	X	C & D	Criminal records information is recorded in CCD for the defendant and victim. This may appear in narrative information. This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	This may be collected or appear in narrative information appear in narrative information for the defendant or victim, if it is relevant to the decision.
Whistleblower, e.g., tip, complaint, or referral	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.

(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
Grand jury information	X	C & D	Information in CCD and its narrative documents are compiled from or for grand jury proceedings.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Procurement/contracting records	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Proprietary or business information	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
Location information, including continuous or intermittent location tracking capabilities	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
<i>Biometric data:</i>			
- Photographs or photographic identifiers	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Video containing biometric data	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Fingerprints	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Palm prints	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Iris image	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Dental profile	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Voice recording/signatures	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Scars, marks, tattoos	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Vascular scan, e.g., palm or finger vein biometric data	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- DNA profiles	X	C & D	This may appear in narrative information for the defendant or victim, if it is relevant to the decision.
- Other (specify)			

(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 Detainees; 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
<i>System admin/audit data:</i>	X	A	This system captured audit data as mandated in National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4. ¹⁹
- User ID	X	A	
- User passwords/codes			
- IP address	X	A	
- Date/time of access	X	A	
- Queries run			
- Contents of files	X	A	
Unanticipated PII		C & D	Given the varied nature of the Division's work, the information placed into this system could include any type of lawfully obtained, unclassified information reasonably determined by the Department to be necessary and/or relevant to the fulsome analysis of a capital case decision.
Other (please list the type of info and describe as completely as possible):			

* For purposes of this chart, "narrative information" refers to the submission package, subsequent legal analysis, recommendations and decisional documents which are uploaded into CCD. These documents are not text searchable in the database.

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

Directly from individual about whom the information pertains

- ☐ In person ☐ Hard copy: mail/fax ☐ Online
☐ Telephone ☐ Email
☐ Other (specify):

Government sources

- ☒ Within the Component ☒ Other DOJ components ☐ Other federal entities
☒ State, local, tribal ☒ Foreign
☐ Other (specify): These sources are relevant to the extent that information obtained from them is relevant to a case.

¹⁹ See <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22>.

Non-government sources

- ☐ Members of the public ☐ Public media, internet ☐ Private sector
☐ Commercial data brokers
☒ Other (specify):
 - Victims and their family members may provide impact statements.
 - The defense counsel is afforded the opportunity to provide input into the decision-making process.

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			Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
	Case-by-case	Bulk transfer	Direct log-in access	
Within the Component	☒	☐	☐	On a case-by-case basis, case specific packages of the information and documents relevant to making a decision will be prepared and provided to members of the AGRCCC or the AG by email.
DOJ Components	☒	☐	☐	
Federal entities	☐	☐	☐	
State, local, tribal gov't entities	☐	☐	☐	
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	The information included in the decision-making process is confidential, and not subject to discovery, however the actual decision to seek or not seek the death penalty will be shared with the defense counsel, victims and their family and the court through the submitting office.
Private sector	☐	☐	☐	

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.
Foreign governments	☒	☐	☐	The information included in the decision-making process is confidential, and not subject to discovery or other sharing, however the actual decision to seek or not seek the death penalty may be shared with involved foreign governments through the submitting office, pursuant to treaty or other cooperative requirements.
Foreign entities	☐	☐	☐	
Other (specify):	☒	☐	☐	Aggregate statistical information could possibly be provided to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, resource requests. Anonymized statistical demographic information could possibly be provided to entities performing authorized studies or audits on the application of the death penalty.

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.*

This information will not be released to the public for “Open Data” purposes. Demographic information is occasionally shared within the Department for statistical purposes concerning Division caseload, activities, performance, and resource requests. Statistical information is anonymized (e.g., no victim or defendant names are disclosed) and aggregated.

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.

The public is provided with general notice of the existence of case files through Division SORN CRM-001, Central Criminal Division Index File and Associated Records last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017).

Generally, individuals are not provided with specific or direct notice of collection about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

However, CCS provides notice to individuals that may be contained within the system, such as victims and witnesses, of the process so that they have an opportunity to provide further information to CCS for inclusion in the AGRCCC and AG reviews.

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.*

The public is provided with general notice of the existence of case files through the System of Records Notice, Central Criminal Division Index File and Associated Records, JUSTICE/CRM-001. Generally, individuals are not provided with specific or direct notice of, or opportunity to participate in the Department's collection of information about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

However, information that the defendant provides as evidence may be included in CCS, and in this instance, CCS provides the defense counsel with an opportunity to provide further information to CCS for inclusion in the AGRCCC and AG reviews.

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.*

Specifically, in this instance, pursuant to the Federal Rules of Criminal Procedure, the prosecution memoranda, death penalty evaluation forms, non-decisional information forms and any other internal memoranda informing the review process and the Department's decision are not subject to discovery by the defendant or the defendant's attorney.²⁰

Information in this system is also exempt from the access, amendment, correction, and notification procedures of the Privacy Act.²¹ Individuals may make access requests for the information maintained in this system via the Freedom of Information Act (FOIA), but such material is generally considered excludable from release as law enforcement sensitive, pre-

²⁰ See Fed. R. Crim. P. 16(a)(2)

²¹ See 28 CFR § 16.91

decisional and deliberative, and/or normally privileged in litigation.²² Such requests will be processed according to the provisions of the FOIA.

Section 6: Maintenance of Privacy and Security Controls

6.1 *The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).*

☒	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): CCD is a subsystem of the Divisions Custom Database Applications System (CDAS) for which the ATO date is April 10, 2025. 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: All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes, are recorded in the Justice Management Division JCAM records. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer. As a matter of security policy, the Division does not release information regarding the existence of POAMs to the public.
☐	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
☒	This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: CCD is rated at an overall moderate level based on the inclusion of litigative and judicial information, specifically related to judicial hearings. The general recommended security categorization for the judicial hearings information type is as follows: • Confidentiality is Moderate • Integrity is Low • Availability is Low The confidentiality impact level is the effect of unauthorized disclosure of judicial hearings information on the ability of responsible entities to conducting a hearing in a court of law to

²² See 5 USC § 552(b)

	settle a dispute. While much information associated with judicial hearings is public, some information is sealed by the court and unauthorized disclosure is punishable by law, fine and/or imprisonment. In the vast majority of cases, unauthorized disclosure of judicial hearings information will have only a limited adverse effect on agency operations, assets, or individuals. Here, none of the special factors which may increase the Confidentiality Impact Determination to High Risk are present. These would include where the life of a victim, witness, or informant may be endangered or where the consequences are likely to endanger public safety.
☒	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: This system undergoes continuous assessments, penetration tests, and vulnerability scans, and is monitored through the CRM IT Security Continuous Monitoring Program. CRM performs vulnerability and configuration management scanning using both tools provided by the DOJ Office of the Chief Information Officer and provided by CRM IT. Continuous monitoring includes the security assessment process and a manual review audit occurs at regular intervals, to the extent required by the National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4.²³
☒	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: The Division collects logs according to the standards in the DOJ Cybersecurity Standards, which include Operating System, Web, Database and Application logs for every FISMA-applicable system. Logs are correlated into appropriate DOJ information systems managed by JMD. Access to these logs is provided to the Justice Security Operations Center, who provided security analysis and log monitoring for unusual activity to the extent required by NIST SP 800-53, Rev. 4. Information Owners and Data Stewards that identify additional audit review requirements per the NIST control selections in their System Security Plan, and further defined by entries in a Continuous Monitoring Implementation Plan (CRM Template), may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the information owner.
☒	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, DOJ-02 and other applicable laws, and as required by DOJ policy.
☒	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: One-on-one training, specific to this system, is conducted for authorized users by the CCS internal system administrator.

²³ See <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22>.

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?*

All Division systems implement technical controls to reduce the risk of compromise to PII. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- CCD has a security categorization of FISMA Moderate and has selected the applicable security controls for a Moderate baseline. The Division will not input any information that would be categorized as “High” under NIST FIPS Publication 199, or NIST SP 800-60, Volume II, into this system without the approval of appropriate privacy and security personnel, to ensure adequate controls are applied to protect such information.
- CCD is accessible by approved CCS employees and Information Technology employees and contractors responsible for upgrades and repairs. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed. It utilizes “tiered,” role-based access commensurate with the end-user’s official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified through the employee’s Personal Identity Verification (PIV) card.
- CCD is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- As described throughout this PIA, all CCD users must complete annual DOJ Computer Security Awareness Training (CSAT) training, as well as read and agree to comply with DOJ information technology Rules of Behavior. CCD system administrators must complete additional system administrator training, which includes security training.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered, role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, CCD’s defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

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.)*

Retention of records within CCD will conform to processes and procedures established by the Division Records Management Section (RMS) for the retention and disposition of media neutral records. CCD records, regardless of the decision rendered, are maintained permanently subject to records retention schedule N1-60-98-4.

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. ☒ 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:*

- o SORN JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007) and amended at 82 Fed. Reg. 24155 (May 25, 2017).
- o SORN JUSTICE/DOJ-002, DOJ Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and amended at 86 Fed. Reg. 132 (July 14, 2021).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Privacy Risk: Unauthorized access or misuse of information

Mitigation: The Division employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. CCD also implements access monitoring, privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

Employee access to CCD is limited based on a need-to-know and the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's PIV card and pin number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by the FISMA. An audit log is maintained of all user logins and actions. Notification of the monitoring is presented clearly when logging into the system.

Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's CSAT training, as well as read and agree to comply with DOJ Information Technology and Privacy Rules of Behavior. This occurs during their orientation upon entering into service with DOJ, and annually thereafter. Finally, CCS provides one-on-one training for employees granted access to CCD. The Division maintains an Account Management Guide and Configuration Management Guide for CCD.

The IT system assessment is documented in the DOJ JCAM assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; administrator access is restricted to the few CCS employees and contractors who administer the program.

Lastly, DOJ published strict guidance on the confidentiality requirements and handling of Capital Cases in the JM.²⁴ This defines the restricted population of the Department personnel who can access the information, the specific routes information can travel, and limits notification of the final decisions to the submitting office. This procedure limits the distribution of CCD information to CCS employees, members of the case specific AGRCCC and the AG. Decisions are relayed directly back to the submitting office, who is responsible for notifying the court and the defense counsel. Thus, information released is the responsibility of the submitting office, who is best positioned to understand the operational security of the immediate investigation as well as any related investigations which may include additional suspects, informants, witnesses, operational or security concerns.

Privacy Risk: Over-collection

Mitigation: Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. CCS must rely on the submitting office to submit the appropriate information to support a fulsome analysis, which by their nature contain deeply personal information. In order to mitigate these concerns, the CCS considered the careful minimization of information collection in the design of CCD's data fields, and proactively provides written and in-person guidance on the submission of the case analysis.

Information that can be standardized and is necessary to support the basic tracking and studies of the capital decision process are done through the mandatory submission forms, which are reviewed and entered into the appropriate data fields by specially trained CCS administrative personnel. This information is gathered through the Death Penalty Evaluation Form and the Non-Decisional Information Form.

As described above, the Non-Decisional Information Form contains demographic information which is collected pursuant to audits and studies of the program which identified and mandated the collection of the information to assess the application of the capital process, but the information is also minimized to only that which is mandated. The information in these forms is reviewed and updated by management to ensure compliance with privacy and security standards. For instance, while law enforcement historically collected SSNs as a means of proper subject identification in the

²⁴ See <https://www.justice.gov/jm/jm-9-10000-capital-crimes#9-10.050>

past, the practice has fallen into disfavor in more recent years due to privacy concerns. In compliance with this concern, CCS has discontinued the collection of SSNs within CCD and removed previously collected SSNs from the system.

The Death Penalty Evaluation Forms are designed to capture only the mandatory standards which must be met to support the final decision. The standards which must be met to justify a capital decision are defined in a check box format. Aggravating factors, mitigating factors and Departmental interests are categorically identified as defined in the JM. In addition to standardized documentation of factors relevant to the decision, this form acts as a guide to help submitting prosecutors evaluate their own case by highlighting the appropriateness of their recommendation.

The crux of the analysis informing the final decision is in the prosecution memo (described in I. 1. e.) and is narrative in nature, thus the information provided is not constrained to defined data fields. Thus, Departmental policy mandates that prosecutors contact CCS at the outset of the capital decision process. CCS takes a proactive role in ensuring that the analysis contains only appropriate and material information. CCS provides and maintains instructions published in the JM as well as extensive reference materials that discuss appropriate information to be submitted on their Intranet site. Additionally, the assigned CCS case attorney will actively work with the prosecutor to ensure the submitted materials are complete and appropriate prior to convening the AGRCCC.

Privacy Risk: Erroneous or inaccurate information

Mitigation: CCS must rely on the submitting office to ensure the accuracy of the information provided. The submitting office has a vested interest in ensuring that the investigative information provided is as accurate as possible. Within the submitting office, an extensive review, including a final decision by the USA or AAG, occurs before a case can be sent to CCS. The inability for the defendant, the victim or the victim's family to directly view the information submitted to CCS eliminates their ability to review or amend the information. To ensure the greatest amount of fairness in the process as possible, CCS ensures that the submitting office affords the opportunity for the victim, their family, and the defense attorney to independently provide statements and input that will be included in the review process. Should information in a submission package be determined inaccurate after a decision by the AGRCCC is made, the information will be reviewed to determine whether it was material to the decision, and whether the AGRCCC and AG need to reassess the case.

Privacy Risk: Information which introduces bias.

Mitigation: CCS's mission is to ensure consistency and fairness in the application of the death penalty. Bias for or against an individual based upon characteristics such as race, color, religious beliefs, national origin, or sex of a defendant or a victim may not play any role in the decision whether to seek or authorize the death penalty, and any influence of passion, prejudice, or other arbitrary factors must be avoided. *See* 18 U.S.C. §§3593(e) and (f) and § 3595(c)(1). At the same time, CCS is required to capture certain demographic information, such as race or ethnicity, pursuant to previous audits and directives, which permit studies of the decision-making process. That information may be characterized as introducing bias into the process. As described above, CCS isolates this information from the assigned attorneys, members of the AGRCCC and the AG, by capturing this information in the Non-Decisional Information form, then withholding the form and restricting access to the associated data in CCD from the CCS attorneys. At the same time, CCS attorneys will leverage their early contact with the prosecuting attorney to discourage the inclusion of bias inducing information that is not

material to the decision from their submission package which could later be transmitted to the AGRCCC and the AG. CCS will request that the submitting office redact any such information that is included in a submission package.