**CIVIL RIGHTS DIVISION**
**Records Requirements Guide for the Creation, Maintenance, and Disposition of Enforcement Records**

*Issued* November 23, 2021

## I. Purpose and Scope

This Records Requirements Guide for the Creation, Maintenance, and Disposition of Records (Guide or RRG) supplements and explains the Civil Rights Division's (CRT or Division) Policy on the Creation, Maintenance, and Disposition of Enforcement Records. The RRG also explains the requirements of the Federal Records Act (FRA) and describes the records that must be included in the file of an enforcement[1] action to document the work of the Division. To support the Division's transition to electronic records management as well as a "media neutral" records schedule, the RRG clarifies the Division's commitment to managing enforcement-related information electronically, within standard folder and subfolder structures in each Section's shared directory (S: drive), and Outlook email accounts. The RRG also provides guidance on the creation, maintenance, and disposition of records and replaces the Division's former "print and retain" policy. The RRG complies with DOJ Policy Statement 0801.06 (Recordkeeping For Litigation Case Files) and applies to all CRT staff[2] who collectively share responsibility for CRT's compliance with the FRA.

While an enforcement action is open, its accompanying files should contain all pertinent records. This includes paper documents, electronically stored information (ESI), and physical evidence needed by the staff working on the enforcement action. Additionally, this includes any records covered by independent preservation obligations, such as litigation holds, stipulations, Freedom of Information Act (FOIA) requests, and court orders. When an enforcement file is closed and any external preservation obligations have ended, the enforcement file should contain only official enforcement records, specifically, those records that demonstrate the substantive nature, course, or outcome of the enforcement action.[3] *See* Section IV, below.

CRT will, to the extent possible, manage all existing and future records electronically. Nothing in this RRG relieves CRT of its obligation to preserve documents, ESI, or physical items in their original format when litigation is reasonably foreseeable. *See* CRT Litigation Hold Guidance, February 24, 2017, for additional information about CRT's preservation obligations

[1] "Enforcement" refers to all cases and matters, as well as any project or initiative, to which the Division has issued a DJ Number. The RRG does not address administrative or non-enforcement files, or other records related to EEO, FOIA, Privacy Act, or litigation that is unrelated to CRT's enforcement activities.

[2] "Staff" and "you" refer to all CRT personnel, including federal employees, contractors, student volunteers, litigative consultants, experts, and individuals working in the Division on a detail, fellowship, or other arrangement.

[3] *See* 44 U.S.C. § 3301, 36 C.F.R. § 1220.18 (providing statutory and regulatory definitions of "records").

and litigation hold procedures. Indeed, Division staff are required to comply with all applicable litigation holds, stipulations, court orders, and statutes, such as *FOIA*, 5 U.S.C. § 552, the Privacy Act, 5 U.S.C. 552a, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g & 34 C.F.R. Part 99, and the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d.

## II. Federal Records Act

The FRA requires all federal agencies to create and maintain records that:

- Document the persons, places, things, or matters dealt with by the agency.
- Facilitate action by agency officials and their successors in office.
- Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.
- Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.
- Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications, or in conference), or electronically. and
- Document important board, committee, or staff meetings.

*See* 36 C.F.R. § 1222.22

The FRA, applicable regulations, and Department policies classify every document you use in your day-to-day work by both the type of record and how long we are required to preserve it. For example, "transitory" documents (*e.g.*, calendars containing filing deadlines) are not considered official enforcement records. Assuming no independent preservation obligation exists other than the FRA, staff should dispose of transitory documents when they are no longer needed for any business purposes. By contrast, a complaint filed in a civil action is an official enforcement record and must be preserved in the enforcement file for a pre-determined period of time (*e.g.*, 3 years, 10 years, 25 years, or permanently) after the enforcement action ends based on the retention period established by the applicable record retention schedule approved by the National Archives and Records Administration (NARA). Division staff must comply with the applicable retention schedule. The DJ classification number (DJ Number) assigned to each enforcement action indicates the applicable record retention schedule for disposition of closed enforcement files. Some enforcement actions have a permanent retention, meaning the custody of the official enforcement file will eventually be transferred to NARA for permanent preservation because of its historical significance. The Division is authorized to destroy official enforcement files that are not designated as permanent only after the retention period expires. *See* Sections V.B., below.

## III. Types of Documents and Records in CRT's Open Enforcement Files

An enforcement file is a compilation of data and documents related to a particular case or matter. An open enforcement file often consists of various documents, including: internal emails, external correspondence, notes, analyses, memoranda, pleadings, orders, witness statements, expert reports, and transcripts, as well as certain administrative records, such as expert contracts. The file also contains evidence obtained during the investigation or discovery, including paper and ESI obtained from complainants, charging parties, victims, witnesses, experts, defendants, third parties, or other government agencies. *See* DOJ Policy Statement 0801.06 (Recordkeeping For Litigation Case Files), section IV (Case File Contents), subsection B (Documentation).

While the enforcement action is open, and assuming no independent preservation obligation exists other than the FRA, the enforcement file will often contain a combination of transitory and/or non-record material. As noted above, transitory documents are needed only for a short time (less than 180 days from the date of creation), and should be properly disposed of when they are no longer needed. This rule applies to all transitory documents, unless CRT is required to retain the document due to independent preservation obligations, such as litigation holds, stipulations, pending FOIA requests, or court orders. At the conclusion of an enforcement action, but prior to closing the DJ Number, the lead attorney working with the other assigned staff is responsible for reviewing and culling the documents within the enforcement file, to ensure the closed file contains only official enforcement records. This process can be expedited by keeping the file organized and labeling, identifying, and isolating official enforcement records throughout the lifecycle of the enforcement action.

## IV. Closed Enforcement File - Federal Record Material

### A. Official Enforcement Records

Official enforcement records include all papers, electronic materials, and other documents (*i.e.*, maps, photographs, video, etc.) made or used in connection with an enforcement action that document the Division's legal and administrative decisions, as well as the Division's actions. In turn, they demonstrate the substantive nature, course, and outcome of the enforcement action. Examples of official enforcement records include:

- Complaints of discrimination that prompt the opening of the case or matter.
- Internal memoranda or communications, including emails and voicemail messages,[4] that recommend or direct actions such as opening, closing, or settling an enforcement action.

[4] All CRT Voice over Internet Protocol (VoIP) phones transfer incoming voicemail messages electronically as a .wav file to the recipient's email. When information contained in a voicemail is pertinent to an enforcement action, the recipient should preserve the message by saving the email with the .wav file attached in the proper email folder in Outlook. *See* Section V.A.4., below.

- Correspondence with external parties documenting the Division's legal and administrative decisions, as well as the significant actions taken by the Division. This includes, for example, emails or letters notifying a potential defendant that an investigation has been initiated, requesting information or discovery, retaining experts, announcing the Division's findings, articulating the Division's legal positions, or proffering a settlement offer.

- Voluntary resolution plans and out-of-court settlement agreements.

- Documents filed with the court and entered onto the ECF docket, including complaints, answers, motions and related exhibits, orders, stipulations, consent decrees, compliance reports, and appeals.

- Disclosures sent to a party pursuant to a court order or the Federal Rules of Civil Procedure, such as witness and exhibit lists and related objections.

- Statements authored or signed by a witness, affidavits, and deposition or hearing transcripts.

- Other working files or drafts that contain unique enforcement-related information and are necessary to demonstrate the substantive nature, course, or outcome of the enforcement action.

Many documents go through several drafts and multiple levels of review before being approved by the Section Chief, the Office of the Assistant Attorney General (OAAG), and/or the Department's senior leadership. Furthermore, parties to an enforcement action may exchange many draft documents and agreements in an effort to resolve a case or matter. However, most preliminary drafts do not contain the types of substantive edits necessary to explain the Division's final recommendation, decision, or action. As such, they are not official enforcement records. Moreover, draft documents that are not submitted to a Section Chief for review or approval are unlikely to be official enforcement records, reflecting the Division's recommendations, decisions, or actions because most substantial enforcement decisions must be approved by a Section Chief or someone delegated with the authority to direct actions by the Department. Thus, the closed enforcement file should contain only a limited number of draft documents, such as an initial settlement offer, the final agreement, and those intervening drafts that memorialize the Division's substantive positions and decisions or draft documents that were submitted to the Section Chief for review and approval.

### B. Other Record Materials

As noted above, an open enforcement file will typically include documents that are not official enforcement records, and should not be retained when the file is closed (including non-record material and transitory documents). *See* DOJ Policy Statement 0801.06, section VII (Non-records and Submitted Material). Such documents are not needed to understand the

substantive nature, course, or outcome of the enforcement action, and must be removed from the closed enforcement file.

Examples of such documents that must be removed from the official enforcement file to prepare the file for closure include:

- Duplicate copies of records.

- Redundant files.

  Some memoranda and correspondence may be drafted with sufficient clarity that it becomes unnecessary to rely on the accompanying record to understand the Division's rationale for making a certain decision or taking a specific action. For example, the text of a memorandum may include a chart summarizing several years' worth of data obtained from a defendant, the text of a letter may summarize an analyst's computations, or an email to a Section Chief may identify the important portions of an investigator's interviews of witnesses. Under these circumstances, it may not be necessary to include the voluminous underlying documents in the closed enforcement file.

- Email, voicemail, and other internal communications between team members and reviewers about the day-to-day conduct of the enforcement action that do not:

  (1) Contain unique enforcement-related information or memorialize substantive enforcement decisions (*e.g.*, emails concerning motions for extensions of time, scheduling and deadlines, discovery disputes, logistical matters, and work assignments); and/or

  (2) Document that a reviewer authorized some substantive decision (*i.e.*, an email from an attorney recommending settlement or enforcement actions or an email from a reviewer authorizing the filing of a motion differ from an email updating the reviewer about an investigative timeline.

- Responses to discovery or information requests, compliance reports, and other materials received by the Division that are not subsequently:

  (1) Marked as a potential exhibit or filed in court.

  (2) Attached to or specifically referenced in a memorandum sent to a Section Chief or someone delegated with the authority to direct some action by the Department; and/or

(3) Attached to or referenced with specificity[5] in a substantive communication to another party to the enforcement (*e.g.*, a letter of findings, an issues letter, notice of objection, or a settlement proffer).

CRT collects and reviews a significant quantity of documents and data during investigations and discovery. However, only these enumerated documents, that the Division relied upon in making its final recommendation, decision, or action, are official enforcement records. Attorneys, for example, may collect and forward to expert witnesses a significant amount of data, but will probably rely on and cite the experts' subsequent reports, not the underlying documents, in their recommendation to the Section Chief. Thus, the expert report is the official enforcement record and the remaining documents should be disposed of at the conclusion of the enforcement action.

- Office of Litigation Support Services (OLSS) documents: Most of the data attorneys and staff provide to OLSS, including information contained in discovery databases, exhibits processed in preparation for a trial, or mapping data, are not official enforcement records. Thus, the lead attorney must consult with OLSS when culling the enforcement file in preparation for closure and coordinate the proper disposition of the of the GIS files, litigation support databases, related applications, and other ESI in their possession. OLSS will manage and subsequently delete / destroy any information not needed by the Section for the closed enforcement file.

- Notes, analyses, charts, calculations, and other "working files" that:

  (1) Are prepared solely for the author's own use and are not shared with a Section Chief, or someone delegated with the authority to direct some action by the Department (*e.g.*, to support an enforcement-related recommendation); and

  (2) Do not contain unique enforcement-related information the Division relied on in reaching a substantive enforcement decision (*e.g.*, witness statements, meeting notes that document an attorney was authorized to take an action).

  Most notes are limited in scope and not fully compiled or properly formulated, and typically the important information contained in the notes will be incorporated into an official enforcement record, such as a memorandum, correspondence, transcript, or pleading. For example, notes taken in preparation for a deposition are normally intended for an attorney's own use, and the deposition transcript is the official enforcement record of what transpired during the depositions.

[5] General references to a large collection of documents (*e.g.*, "After reviewing the documents you provided to us on January 15, 2020 in response to our request for information, we…") does not provide sufficient specificity to warrant retention of the entire production.

- As indicated above, drafts that are not submitted to a Section Chief, or someone delegated with the authority to direct some action by the Department, are unlikely to be official enforcement records reflecting the Division's recommendation, decision, or action. Similarly, draft settlement agreements should not be included in a closed enforcement file unless they contain substantive edits necessary to explain the Division's final recommendation, decision, or action.

- Files received from other Federal Agencies (*e.g.*, OCR, EEOC, HUD, FBI), should be returned to that Agency or, if the Agency confirms the files are copies, destroyed at the Agency's request.

- Administrative records, such as travel authorizations, expert witness contracts, invoices, and documents related to other litigation expenses that are maintained by CRT's Administrative Management Section (ADM). Although it may be appropriate to store copies of these records in an open enforcement file to ensure they are preserved when an enforcement action is likely to last longer than the administrative record retention schedule period (typically six years), the records should not be placed in the closed enforcement file.

- Calendar entries, notifications, and other scheduling records that concern work-related trips. Various meeting types, such as interviews, depositions, settlement conferences, settlement meetings, team meetings, staff meetings, or docket reviews also should be removed from the closed enforcement file.

- Files or task lists intended as a reminder that an action is required or expected on a given date. This includes actions and reminders used to track deadlines for production, or receipt of discovery documents, and court filing deadlines.

- Personal papers of a private or non-official nature that do not relate to an enforcement action. Such documents should be maintained separately from official enforcement files. If a document contains such personal information and information about an enforcement action, the document should be copied with the personal information deleted.

- Blank forms and library materials.

- Routing slips and transmittal sheets.

## V. Procedures for Creating, Maintaining, and Closing CRT's Enforcement Files

To comply with the requirements from the Office of Management and Budget, CRT has transitioned to electronic records management. As a result, CRT's official enforcement records will no longer be printed and retained in paper form and stored at the Federal Records Center (FRC). Instead, all enforcement records, including emails, word processing files, PDFs, spreadsheets, and video/audio files, will be stored electronically: (1) in the Sections' S: drive

folders or (2) users' Outlook email accounts.[6]

Consistent with best-practice rules, each Section will create protocols concerning: (1) scanning, uploading, authenticating, and maintaining documents that are needed while an enforcement action is open; (2) folder structures and naming conventions for S: drive documents and emails; (3) version control and document indexing and tracking; (4) record restriction, preservation, and deletion; and (5) file culling, transition, and storage of long-term records. Each Section also will establish mechanisms to ensure that staff comply with applicable policies and that all enforcement files are properly preserved, well-organized, and readily accessible to the appropriate staff. All staff on each enforcement action are required to comply with this RRG and seek guidance from Section management if you have any questions on how to implement these requirements.

To encourage consistent practices, the Division has developed an illustrative standard folder and subfolder structure for S: drive enforcement files. Section Managers may contact the Division's Records and Information Management (RIM) Program Team and the Office of Information Technology and Cybersecurity (OITC) through the CRT Help Desk for advice on preparing or revising their policies and assistance designing their folder structure. The RIM Program Team and OITC also are available to answer questions regarding, for example, scanning and uploading documents; storing records on thumb drives or other physical format; implementing preservation protocols and/or restricting access to folders; authenticating documents; creating discovery databases; and using collaboration programs and file sharing systems (*e.g.*, JEFS); etc.[7]

## A. Creating and Maintaining Enforcement Files

### 1. DJ Numbers

To organize and manage case files, CRT uses a classification system that assigns a specific three-part DJ Number to every matter, *see* DOJ Policy Statement 0801.06, section II (Case File Numbering), subsection A (Assigning DJ Numbers). An example of a DJ Number is "169-33-72." The first part (169) identifies the subject matter or statute at issue in the matter or case. This also identifies the applicable record classification and record retention schedule for the enforcement files. The second part (33) corresponds to one of the 91 judicial districts where the case or matter arose. The third part (72), represents the sequence of matters/cases in that

[6] Section managers may authorize some open enforcement files to be stored on designated discovery databases, such as Relativity, especially documents received during discovery that are not likely to be included in the closed enforcement file. CRT also may authorize the use of certain collaboration software programs for enforcement purposes, and will establish policies for the use of such tools. However, you should consider the potential risks of using these programs and maintaining records in such locations, and ensure that all material that must be included in closed enforcement files are placed within an appropriately designated folder on the Section's S: drive or an email folder in Outlook at the conclusion of the enforcement action.

[7] Section staff also may confer with OLSS staff to discuss some of these topics as they arise in individual cases, and they are encouraged to consult with their Section's E-Discovery Office Coordinator(s) (EDOC) about the discovery implications of certain policies and practices.

jurisdiction. Assigning a DJ Number is the first step to creating an enforcement file. Each Section has an individual who has primary responsibility for assigning DJ Numbers (*e.g.*, case management specialist), and all staff are required to track and maintain all enforcement files using the applicable DJ Number and any other unique identifiers required by each Section's protocol (*e.g.*, case name).

The Section that opens and assigns a DJ Number to an enforcement action is considered the custodian of the official enforcement file, and the same DJ Number should be used if multiple Sections work on the same enforcement action. When an enforcement action is open, the assigned staff should maintain their records in accordance with their Section's policies. When the enforcement action closes, the assigned staff must coordinate to ensure the custodian Section's closed enforcement file is complete.

### 2. Receipt and Scanning of Records

CRT's record policy requires you to obtain and maintain all records related to an open enforcement file electronically whenever feasible, consistent with applicable rules of evidence and preservation policies. All closed enforcement files must be maintained electronically unless they are specifically exempted from this RRG. *See* Section V.B.4., below.

Accordingly, you are encouraged to collect records and evidence as ESI, and, whenever feasible, witnesses and defendants should be instructed to produce documents and evidence electronically. Sections will develop policies concerning the scanning and storing of documents we receive in paper format, as well as the uploading of ESI received on data storage devices (*e.g.*, DVDs, thumb drives, etc.), maintaining data storage devices, and the downloading and authenticating of ESI we receive from file sharing systems.

All enforcement-related paper documents that can be accurately converted to ESI must be scanned upon receipt and the electronic copies should be placed on the S: drive.[8] Similarly, ESI that can be safely uploaded and stored on our network should be placed on the S: drive in a timely and proper manner. You should be familiar with the Department's Cybersecurity and Privacy Rules of Behavior and you should consult OITC through the CRT Help Desk and OLSS to ensure you are familiar with the current protocol for receiving ESI from an external source. You should also take precautions when using file sharing software to exchange documents. Some file sharing software may not protect personally identifiable information (PII), may delete files after a certain period of time, and may have complex document quarantine protocols.[9]

---

[8] As noted above, some files may be stored in a litigation support database in lieu of the S: drive in accordance with the Sections' policies.

[9] Sections are encouraged to consult with their EDOCs, OITC, and OLSS and develop guidance for the use of technologies, such as collaboration tools, that may impact how the Section conducts discovery. For example, you may need to take proactive steps to ensure documents received via file sharing software can be authenticated (*e.g.*, independently verify documents' hash values) because such discovery exchanges may prevent us from having the "original" document or data storage device.

You are required to scan and upload all portions of files received from other Federal Agencies, including referral files (non-CRT Agency Records), that CRT needs to conduct enforcement actions.[10] You are also required to download to the S: drive all enforcement-related records created or collected using other devices, such as pictures on iPhones in a timely manner.[11]

Documents that cannot be accurately retained electronically and ESI that cannot be safely uploaded or properly stored on the S: drive, may be kept in their original format and should be stored in the Section's file room or some other organized and secure location. *See* Section V.A.5., below.

### 3. Creating and Maintaining Electronic Enforcement Files in the Section's Shared Drive

When a Section opens and assigns a DJ Number to a new enforcement action, the case management specialist should create an enforcement folder within the Section's S: drive. The file name must include the DJ Number followed by any other unique identifiers required by Section policies.[12] The file also must include all subfolders and all overwrite/access restrictions required by Section policies.

After the appropriate enforcement folder is created on the S: drive, you must place and maintain all enforcement-related records in the designated S: drive folder in accordance with Section protocols, naming conventions, and best practices to ensure records are properly preserved, well-organized, and readily accessible to the appropriate staff. As noted above, each Section will institute measures to ensure files are organized in accordance with this RRG.

You should not create or save any enforcement-related files in your home directories (H: drives[13]). You may only use the H: drives for personal records, such as performance reviews, docket review memos, or other administrative material. After the Sections have migrated

---

[10] CRT's enforcement files should include only copies of non-CRT Agency Records that we need to perform our enforcement actions. *See* Section IV.B., above. After scanning such documents, you should preserve the original file in its "as-received" format until CRT closes the enforcement action to which the file relates. *See* Section V.A.5., below.

[11] You should confer with the OITC and OLSS if they have any questions about properly preserving ESI with the associated metadata that may be relevant to their case. You also may preserve the original versions of such records on their iPhones or other devises until they are no longer needed.

[12] Sections may use an automated script that allow individual users to create shortcuts in their files that they can re-name as they see fit, so long as the official file on the S: drive comports with CRT and Section naming conventions. This allows the Division's files to be organized in a uniform, easily searchable manner while facilitating assigned staff's easy access to the folder location because they will see only the enforcement files that work on and they will be able to readily identify them.

[13] The Division will move toward using OneDrive either in place of or in parallel with S: and H: drives.

enforcement records onto the S: drive, H: drives will have size limitations and will be accessible only to the individual user, a Section Chief or Principal Deputy Chief and, at the Section Chief's discretion, one or more Deputy Chiefs. You should also not create or save enforcement-related files on the C: drives of their laptops. Finally, as noted above, you should ensure that any enforcement-related records that you create or collect using other devices (*e.g.*, iPhone pictures) are transferred to the S: drive in a timely manner.

Consistent with Section policies, all staff should be familiar with basic knowledge management principals and adopt best practice techniques. For example, you should:

- Minimize the creation and use of duplicate records, which increases the burden and expense of preparing discovery and FOIA responses and makes it more difficult for the staff to cull and close enforcement files.

- Label folders/files in an organized and consistent fashion (*e.g.*, distinguish drafts from final versions, identify the record copies of documents that contain reviewers' PIV card authorizations, use dates in filenames, utilize existing file system like the ECF Docketing Numbers, and adopt uniform version control measures, etc.).

- Identify and isolate official enforcement records throughout the lifecycle of the enforcement action so records that must be included in the closed enforcement file are distinguishable from transitory documents that must be culled when appropriate.

- Identify and isolate documents that are sensitive and should not be accessible in the common enforcement file (*e.g.*, documents that must be screened by independent privilege review teams).

- Identify and, where appropriate, isolate documents that contain PII or records that must be disposed of pursuant to independent authorities, such as FERPA or HIPPA.

- Use document logs to track documents received or produced during investigations and discovery.

- Maintain documents received through investigations and discovery in their original "as-received" format, and trace the origin of subsequently created documents used for analytical purposes (*e.g.*, do not filter or sort original Excel files and create "save as" files before altering original photographs).

- Periodically review the assigned enforcement files to ensure they are well-organized and properly maintained.

- Comply with applicable record retention schedules and delete all transitory documents when they are no longer needed and you are authorized to do so (*i.e.*, periodically if allowed under the Rule 26(f) Stipulation, when a litigation hold is lifted, or when the case ends, etc.).

OITC is available to help Sections update their individual policies, upgrade their S: drive structure, and migrate files as needed. OITC also is developing proposals to modify user restrictions and enhance CRT's file preservation and protection protocols.[14] Section Managers may contact the CRT Help Desk to inquire about this initiative. Individual staff also should contact the CRT Help Desk immediately if you discover that any files have been mistakenly moved or deleted from their enforcement files.

### 4. Creating and Maintaining Enforcement Email

In addition to the S: drive enforcement file, all staff must create a folder for each of their assigned enforcement actions in their Outlook accounts that includes the DJ Number. All emails concerning the enforcement action, including related voicemail messages sent to email accounts as .wav files, must be placed in that case or matter specific folder or subfolders.

Consistent with Section policies, you should adopt best practice techniques for the use of emails. For example, you should:

- Clearly identify all enforcement-related emails in the subject line by adopting a uniform case- or matter-specific identifier to be used by all staff assigned to the enforcement action. This may include the DJ Number or some other short, Section-approved identifier that will enable users (or OITC and OLSS) to quickly search all email files and locate emails that relate to specific enforcement matters and may be subject to future production, disclosure, or retention.

- Consider using subfolders to identify and isolate substantive emails that are official enforcement records and must be retained in the closed enforcement file apart from other transitory emails that should be deleted when they are no longer needed and you are authorized to do so. You may also use similar techniques to isolate emails that contain PII or are subject to other preservation of destruction rules (*e.g.*, FERPA).

- Consider identifying one team member as the record custodian to be copied on all enforcement-related emails. This increases the likelihood that one individual will have a complete record of all communications related to the case or matter. It also reduces the burden and expense of preparing discovery and FOIA responses.

- Use hyperlinks and other tools that reduce unnecessary document duplication (*e.g.*, attaching a draft motion already located in the enforcement folder on the S: drive to an email creates additional copies of that document in one's Outlook sent folder and the Outlook inboxes of every recipient of that email).

- Periodically review your Inbox and Sent emails to ensure all enforcement-related emails are placed in the proper folders. You are reminded that all mail is stored on

[14] Some of these modifications may limit the number of people who may move or delete a file while allowing more people permissions to open and review them, thereby reducing the risk of documents being accidentally deleted.

the server. Typically, however, only the past several months of mail is visible in Outlook. Searching for email in Outlook or clicking to view more on Microsoft Exchange will expand all results.

- Comply with applicable record retention schedules and delete all transitory emails when they are no longer needed and you are authorized to do so (*i.e.*, periodically if allowed under the Rule 26(f) Stipulation, when a litigation hold is lifted, etc.).

- Comply with Department policies prohibiting the use of personal or non-official email accounts to send communications related to official business, except in exigent circumstances.

CRT's current email system has a permanent retention policy. Files are not deleted automatically, but must be deleted manually by each user. If CRT amends its retention policy in the future, OITC will notify all staff and help the Sections implement record retention policies. Individual staff also may contact the CRT Help Desk if you discover that any emails have been mistakenly moved or deleted from their enforcement folder.

### 5. Maintaining Paper Records, Evidence Subject to a Litigation Hold, and Other Media

As noted above, CRT's record system requires you to maintain all records related to an open enforcement action electronically whenever feasible and documents that can be accurately converted to ESI should be timely scanned for day-to-day use and inclusion in the closed enforcement file. At the same time, you must also comply with all applicable rules of evidence and preservation policies, and some records must be retained in their original "as-received" format after they are scanned or uploaded to the S: drive, so they may be properly authenticated in any future legal proceeding.

Documents that cannot be accurately retained electronically and ESI that cannot be safely uploaded or properly stored on the S: drive (*e.g.*, due to size or security limitations), may be kept in their original format and should be stored in the Section's file room or some other organized and secure location. Some portions of an enforcement file also may be specifically exempted from scanning (*e.g.*, oversized documents that cannot be scanned), and the case management specialists will coordinate with the RIM Program Team to address the storage of these records on a case-by-case basis.

The original versions of all records that have potential evidentiary value, as well as all non-CRT Agency Records and all records that are subject to a litigation hold, must be preserved in their original "as-received" format after they are scanned or uploaded, until the parties to the enforcement action have reached a stipulation regarding the preservation or authenticity of the documents, any litigation hold is lifted, or the enforcement action is closed. The electronic copies of such records should be placed on the S: drive for day-to-day use and eventual inclusion in the closed enforcement files while the original versions are maintained in the Section's file room or other secure location.

You should also preserve all enforcement-related data storage devices, including all DVDs and thumb drives, in their original condition to ensure their content can be properly authenticated should the need arise. As noted above, each Section will establish polices to ensure these devices are labeled clearly and stored safely until they can be properly overwritten and recycled when they are no longer needed and you are authorized to dispose of the records. You are required to timely download to the S: drive all enforcement-related records that you create or collect using other devices (*e.g.*, iPhone photos). However, you may continue to preserve the original versions until such time as they are no longer needed and you are authorized to dispose of them.

Each Section will develop policies concerning the storage of paper files in the Section's file room, in collaboration with the RIM Program Team and all other Sections that share the same space. These policies will establish the rules for accessing file rooms, placing and removing files, labeling, and organizing files, maintaining over-sized documents, safeguarding data storage devices, etc.

## B. Closing and Preserving Enforcement Action Files Under the Record Retention Schedule

### 1. Record Retention Schedules and Federal Record Centers

As noted above, the Department's record classification system assigns a DJ Number to every enforcement action, which corresponds to a particular record retention schedule that indicates if and when CRT may dispose of the enforcement file after the case or matter closes. *See* Section II, above. An enforcement file is either "temporary" and CRT must preserve it for a pre-determined period of time (3 years, 10 years, or 25 years) or "permanent" and CRT must eventually transfer it to NARA.[15]

Previously, CRT would "print and retain" enforcement files that were then transferred to the FRC for safe storage for the applicable retention period, the time between when the enforcement file was closed and the appropriate disposition date. During the retention period, an enforcement file remains in the care and custody of CRT. FRC would contact the RIM Program Team on the disposition date to determine whether the file should be destroyed or transferred to NARA. In addition, CRT's records management policy anticipates the use of the FRC being eliminated in the future as a repository to store analog records. Those will be maintained on CRT's computer servers.[16]

---

[15] Currently, the majority of CRT's closed enforcement files are classified as historically significant and are considered permanent records. Although CRT may create new DJ Numbers under the existing classification system, it cannot change the classification system or the corresponding record retention schedules without approval from NARA and the Department's Office of Records Management Policy (ORMP).

[16] You will still be able to request the return of files that were previously transferred to the FRC, and are being stored there for the remainder of their retention period, if those files need to be retrieved for any reason (*e.g.*, to respond to FOIA requests), and should confer with their Section's case management

When the enforcement action concludes, you must prepare the closed enforcement file by compiling and organizing all official enforcement records and culling out all non-record materials. *See* Section IV., below.

### 2. Closing Electronic Enforcement Files on Shared Drive

When an enforcement action concludes and all other preservation obligations other than the FRA (*e.g.*, litigation holds) end, the lead attorney must ensure that all ESI related to that action is reviewed, culled, and placed into proper folders and subfolders on the S: drive and that the closed enforcement file:

(a) Contains all electronic enforcement records necessary and appropriate for inclusion in the closed file, except for email correspondence and other records retained in Outlook; and

(b) Does not contain any transitory or non-record material that should not be included in the closed files

*Compare supra at* part IV A. *with* B.

Preparing a closed enforcement file will require you to identify and retain the records needed to understand the substantive nature, course, or outcome of the enforcement action, and to delete all other items that should not be retained in the official enforcement file. Before organizing the S: drive file, the lead attorney must coordinate with every individual who worked on the enforcement action and may have records that should be included in the closed enforcement file. *See* Section V.B.4, below. For example, a lead attorney should coordinate with Section Managers to ensure that the closed enforcement file includes any official enforcement record the reviewers may have placed outside the designated enforcement folder on the S: drive. Lead attorneys must ensure that the closed enforcement file contains only one copy of each enforcement record by deduplicating and deleting all copies. Finally, they must ensure that all transitory and non-record materials are deleted.

Consistent with Section policies, if the assigned staff believes a convenience copy of certain documents from their enforcement actions should be retained elsewhere in the Section's S: drive for future instructional purposes and easy access (*i.e.*, template/sample motions), you should confer with their Section Management about how to copy those particular files and where to place them. Whenever possible, such documents should be modified/redacted to distinguish them from enforcement files.

The lead attorney, and the Section Records Liaison, or other individuals designated by Section Leadership are responsible for inspecting closed enforcement files to ensure they are properly culled and organized. Once the inspection is completed, the lead attorney will notify

---

specialist on how to do so.

the Section's case management specialist that the file is ready for processing for records purposes. The case management specialist will then record the applicable disposition date,[17] index the files, and coordinate with the CRT Help Desk and RIM Program Team to ensure the entire closed enforcement file is transferred to a secure "archival" server location for the duration of the applicable retention period. Access to this archival folder will be limited to read-only for most staff, and may be further restricted pursuant to Section protocols.

### 3. Closing Enforcement Action Email

When an enforcement action concludes and all other preservation obligations other than the FRA (*e.g.*, litigation holds) end, the lead attorney must ensure that all email correspondence and other enforcement-related records retained in Outlook is reviewed, culled, and placed into folders labeled with the applicable DJ Numbers in the custodians' Outlook accounts. This process should ensure that the remaining folders:

(a) Contains all Outlook emails, .wav files, etc. that are necessary and appropriate for inclusion in the closed file; and

(b) Does not contain any transitory or non-record material that should not be included in the closed files.

*Compare supra at* part IV A *with* B.

Preparing closed enforcement files in Outlook will require assigned staff to identify and retain the email communications and voicemail messages needed to understand the substantive nature, course, or outcome of the enforcement action, and to delete all other items that should not be retained in the official enforcement file. Lead attorneys also must coordinate with their reviewers and Section Chiefs to ensure that their Outlook files are similarly culled and that all official enforcement records are identified and isolated for inclusion in the closed enforcement file (*e.g.*, emails between the Section Chief and OAAG personnel).

As noted above, staff can employ different strategies during the life of the enforcement action to ensure all email correspondence that are official enforcement records can be readily identified and placed in the closed enforcement file (*e.g.*, identifying email custodians) and the labor involved in culling the file can be reduced. The case management specialist and lead attorneys also may contact the OITC Help Desk to discuss the use of various document review technologies that may help them identify emails that need to be retained, deleted, or methods to reduce duplicates.

Consistent with Section policies, if the assigned staff believes a convenience copy of certain email should be retained for future institutional purposes and easy access, you should

[17] The RIM Program Team will devise a uniform system for monitoring disposition dates throughout CRT and will work with each Section's case management specialist to determine what documents need to be included in the index and any accompanying memo.

confer with their Section Managers about where to store those particular emails. Whenever possible, such items should be relabeled, in order to distinguish them from enforcement files.

Once the relevant Outlook files have been prepared and reviewed, the lead attorney will notify the Section's case management specialist who will then record the applicable disposition date, index of the files, and coordinate with the OITC Help Desk and the RIM Program Team to ensure the relevant Outlook files are transferred to a secure "archival" location for the duration of the applicable retention period. After the necessary emails are transferred and the closed enforcement file has been properly stored, all staff who worked on the case or matter should delete their email folders for that DJ Number.

### 4. Closing Enforcement Files Not Stored on Shared Drive or Email

When an enforcement action concludes and all other preservation obligations other than the FRA (*e.g.*, litigation holds) end, the lead attorney must identify and locate all enforcement-related files that need to be reviewed and either included in the closed enforcement file or deleted, which may require the lead attorney to coordinate with a number of different individuals who may have such records.

The following are some of the steps the lead attorney may need to take:

- Notify the reviewers within the Section when you anticipate closing an enforcement action so they can prepare their files for potential inclusion in the closed enforcement file.

- Inspect Section's file room and all data storage devices for files that may need to be included in the closed enforcement file. If these files were previously scanned/ uploaded to the S: drive and/or they do not need to be included in the closed enforcement file, the lead attorney should coordinate with the Section's case management specialist to dispose of the files and recycle the data storage devices in a proper manner.[18]

- Coordinate with the case management specialist and RIM Program Team concerning the long-term storage of all portions of the closed enforcement file that are exempted from scanning (*e.g.*, oversized documents).

- Inspect the S: drive "gone" folders of former CRT Section employees who may have worked on the enforcement action and kept files on their H: drives. The lead attorneys also may need to have their reviewers contact the OITC Help Desk to initiate a review of the former users' Outlook accounts.

[18] CRT still utilizes "burn boxes" to dispose of various files, as well as large recycling bins for paper files. The Case Management Specialist also may send data storage devices to either the OITC Help Desk or OLSS to have the data properly scrubbed and the media recycled.

- Ask all staff who worked on the enforcement action to inspect their H: drives and any other locations where documents may be stored, and to move the relevant files to the proper location on the S: drive.

- If applicable, notify the referring Agencies, the USAO, other Department components (*e.g.*, Office of the Solicitor General), and all litigating consultants and expert witnesses and inform them that the enforcement action has concluded and coordinate with them to facilitate the collection or disposition of all relevant records.

- Notify all other Sections and Offices within CRT that worked on the enforcement action (*e.g.*, APP, OAAG, or OLSS) and coordinate with them to facilitate the collection or disposition of all relevant records. As noted above:

    - All Division staff must cooperate to ensure the custodian Section's closed enforcement file is complete.

    - While most OLSS records and discovery databases will not be included in the closed enforcement file, the lead attorney should confer with OLSS when an action concludes to determine what records they have and enable OLSS to delete the applicable files and reclaim space on the relevant computer servers.

- Ensure that all non-CRT Agency Records are returned to that Agency or disposed of at the Agency's request.

As noted above, enforcement-related paper documents should be scanned upon receipt, and the lead attorney should ensure than any paper files located in the file room that were not scanned and need to be included in the closed enforcement file are scanned and placed on the S: drive. If the lead attorney identifies any paper files that need to be included in the closed enforcement file that cannot be scanned or downloaded (*e.g.*, oversized documents), the lead attorney must notify the Section's case management specialist who in turn will coordinate with the RIM Program Team to ensure the files are stored properly for the duration of the applicable retention period.

### 5. Specialized Procedures for Handling Sensitive Information

Federal law mandates that certain documents or other information obtained during an enforcement action require specialized handling. In addition to the Privacy Act that affects all Sections, there is grand jury material under the Federal Rules of Criminal Procedure, and documents subject to the FERPA, HIPAA, and the Right to Financial Privacy Act (RFPA). In some circumstances, information or documents may also be subject to a protective order, filed under seal, or involve classified materials.

All staff assigned to any enforcement action implicated by one of these obligations must pay careful attention to isolating the appropriate information or document(s), limiting access to authorized personnel during the pendency of the enforcement action, and following the appropriate retention or destruction processes. Although Sections retain discretion to craft their

individual records protocols in the manner that suits their business practices, the Sections' policies must comply with the following:

**Privacy Act:** CRT's enforcement activities often result in the acquisition of PII about individuals, including names, identifying numbers, symbols, and other identifying information, such as educational, financial, medical, criminal, and employment data. The Privacy Act requires Department staff to collect only such information as is authorized; limit its use; minimize its proliferation; and secure it from unwarranted disclosure. Each Section shall consult with the RIM Program Team and OITC in developing their procedures, particularly with regard to PII that may be maintained in connection with enforcement actions that have been closed. Once completed and prior to their implementation, Sections shall obtain the concurrence of the Freedom of Information Act/Privacy Act Office and the Executive Officer with regard to the protocols.

**Grand Jury Materials:** Federal Rule of Criminal Procedure 6(e) requires that all "records, orders, and subpoenas relating to grand-jury proceedings must . . . be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury." The Department staff necessary to enforce federal criminal law shall maintain the secrecy of grand jury proceedings. *See* Fed. R. Crim. P. 6(e)(2) and (3).

When an enforcement action is open, Rule 6(e) materials that exist in hard copy must be stored in authorized locked containers or vaults and electronic Rule 6(e) materials must be stored in a clearly marked subfolder. Regardless of format, access to this material must restricted to those staff identified on the 6(e) list for that specific enforcement. When an enforcement action is closed, grand jury materials must be retained in the clearly marked archival grand jury subfolder with appropriate access restrictions. When another Section wishes to review 6(e) records in a related or parallel proceeding, the affected Section Chief shall consult with CRT's Criminal Section to determine the legal requirements for seeking access to material protected by Rule 6(e).

**Federal Education Rights and Privacy Act:** FEPRA establishes a stringent framework for the receipt, dissemination, and disposal of personally identifiable information contained in education records and covered by the statute (student PII).

- Student PII can only be handled by or disseminated to certain authorized representatives of the Attorney General;

- All authorized representatives must maintain student PII in a manner that will not permit the personal identification of students or their parents by any unauthorized person; and

- Student PII must be destroyed when CRT no longer needs it for auditing or evaluating Federal- or state-supported education programs or enforcing Federal legal requirements related to such programs (*i.e.*, "enforcement purposes").

*See* 20 U.S.C. §§ 1232g(b)(1)(C); 1232g(b)(3); 34 C.F.R.§ 99.35(b)(2). Staff who handle, disseminate, and dispose of student PII covered for enforcement purposes must store the records containing the student PII in a secure and organized manner that protects it from further disclosure or unauthorized use and you must refrain from disseminating student PII to anyone who is not authorized to see it.

Except for documents enumerated below, which are federal records that must be retained in the closed enforcement file, all other documents or records received from an education agency, including all documents received in responses to discovery, information requests, and compliance reports, should be destroyed when they are no longer needed for CRT's enforcement purposes, but no later than when the enforcement action is concludes and the enforcement file is closed.

With respect to FERPA-covered federal records that were:

(a) Used as an exhibit (in a deposition, motion, or hearing).

(b) Attached or referenced with specificity in a memorandum sent to a Section Chief or someone authorized to approve some action by the Department. and/or

(c) Attached or referenced with specificity in a substantive communication to the school district or another party to the enforcement (*e.g.*, a letter of finding, an issues letter or notice of objection, a settlement proffer).

You will redact all the student PII on the record when the information is no longer needed for enforcement purposes, and before such records are placed into the closed enforcement file. If a line-by-line redaction of the student PII is overly burdensome, you may delete the entire document containing the PII and substitute it with a short memorandum in the closed enforcement action file, describing the information that was removed and the reason for removing it.

**Health Insurance Portability and Accountability Act:** Compliance with HIPAA can be achieved in the same manner as FERPA.

**Right to Financial Privacy Act:** This Act implicates individually identifiable financial records of financial institution customers. It provides for the release of records by financial institutions pursuant to customer authorization, administrative or judicial subpoena, search warrant, or formal agency request. As with the protections related to PII, you must take all steps to protect such information from unwarranted disclosure and to limit access to only authorized personnel.

**Protective Order & Sealed Records:** During the pendency of an enforcement action, electronic documents subject to a protective order or filed under seal will be saved according to Section protocols with access limited to authorized staff. For those documents that are not deleted or destroyed by court order when the enforcement action is completed, the Section's case management specialists will coordinate with the RIM

Program Team to ensure the folders containing the covered files and the accompanying record indexes are appropriately labeled to indicate that they contain restricted information.

**Classified Materials:** CRT enforcement actions rarely involve the need to review or handle classified materials. Should such a situation arise, the reviewer overseeing the enforcement action, along with the Section's case management specialists and lead attorneys, shall contact the RIM Program Team to develop policies for the handling and disposition of the classified materials.

### 6. Final Disposition of Enforcement Files

Closed enforcement files will remain in the appropriate archival file location(s), until their disposition date, as mandated by the applicable records schedule.

When a closed enforcement file reaches its disposition date, the Section's case management specialists will coordinate with the RIM Program Team to either dispose of the files or transfer the permanent files to NARA. The RIM Program Team is working with ORMP and NARA to coordinate this process with the Sections' involvement.

## VI. Capstone

In accordance with DOJ Instruction 0801.04.04 (Records Closeout and Processing for Capstone Officials), specifically section II (*Background*, see second paragraph), "DOJ uses the Capstone approach for the capture of all business records as a record series from officials at or near the top of an agency (or an organizational subcomponent). Capstone records are scheduled and preserved as permanent."

Accordingly, CRT has designated the Assistant Attorney General, Principal Deputy Assistant Attorney General, Deputy Assistant Attorneys General, Director of Operational Management, Chief of Staff, Senior Counsels and all career and non-career employees in the OAAG (whether acting, on detail, or otherwise temporary performing these roles) as Capstone officials, whose official records and email accounts will be retained as permanent, historically significant records.

As this relates to CRT, when a Capstone Official leaves the Division, the Front Office (FO) staff, with guidance from the RIM Program Team, is responsible for organizing and securing his or her record information for proper management, storage, and disposition according to federal requirements. In turn, all email contained in their email accounts will automatically be retained as long-term records, including emails deleted by the user.

Individual portions of this guidance, involving the planning and implementation tasks, may be delegated or designated to FO staff. However, the AAG maintains ultimate responsibility for the Division meeting all of its Capstone implementation requirements.

## VII. Roles and Responsibilities

All CRT staff have an important function to perform in the lifecycle and management of most enforcement files (*e.g.* creating, maintaining, and closing):

### A. Section Managers

Section Managers are responsible for maintaining all Section files, ensuring Section staff comply with this RRG, and ensuring the Section adopts and implements a records policy that addresses each of the following:

- Adopting a Section-level RIM Policy;
- Procedure for requesting and obtaining a DJ Number;
- Practices for ensuring open enforcement files are retained in an organized, accessible, and secure manner (*i.e.*, folders structures, naming conventions, deduplicating records, scanning protocols, etc.);
- Practices for storing enforcement-related emails;
- Practices for storing enforcement-related electronic materials on the S: drive;
- Procedure for delegating responsibility for maintaining open and closed enforcement files to a specific individual;
- Procedures for closing enforcement files; and
- Protocols for communicating with OITC and the RIM Program Team.

### B. Assigned Staff

While an enforcement file is open, all staff assigned to the enforcement action are responsible for complying with this RRG, as well as the requirements of their Section-level RIM Policy. This includes policies for disposing of transitory records and ensuring long-term records are properly maintained in Outlook and S: drive folders, and any original hard copy or media are properly and securely stored.

When an enforcement action concludes, attorneys are responsible for reviewing all enforcement-related emails, ESI, and any hard copy documents to ensure the enforcement file contains only official enforcement records. Once that task is completed, professional and support staff are responsible for coordinating with their Section's case management specialists and OITC to move the closed enforcement file to the proper archival locations for preservation in accordance with the applicable record retention schedule.

### C. Section RIM POCs

Section RIM POCs are required to work with the Division's RIM Program Team to resolve any policy questions/issues related to both open and closed enforcement files. Section RIM POCs also are responsible for preparing records for long-term storage and archiving of files in accordance with their record retention schedules, and for transferring all permanent closed enforcement files to NARA (*i.e.* making sure they are in an appropriate NARA approved file type).

### D. Administrative Management Section

ADM is responsible for creating, setting and training on the CRT RIM policy, encompassing proper Records Lifecycle Management (*e.g.* records creation, maintenance, and disposition). ADM also is responsible for ensuring that CRT's policies are periodically reviewed and updated to ensure compliance with DOJ and NARA standards.

### E. Division Records and Information Management Program Team

The RIM Program Team is responsible for retiring hard copy closed enforcement files to the FRC, and then assisting with Reference Requests *(i.e.* obtaining subsequent access to them). With the support of OITC, the RIM Program Team will work with Section records liaisons to ensure the official enforcement files are deleted/destroyed upon reaching their disposition date, and permanent enforcement files (electronic and any hard copy files), which are historically significant, are prepared appropriately for accession into the Archives.

The RIM Program Team serves as the Division's liaison to ORMP, the FRC, and as needed, to NARA. The RIM Program Team also coordinates Section-level reviews and approvals for records that have reached their disposition date, and are therefore eligible for destruction (temporary), and/or accession (permanent) into the Archives. They also provide advice, guidance, and support to Division management, which is consistent with the FRA, relevant regulations, and laws.

## VIII. Departing Employees

Each Section shall establish a protocol for all departing employees, including employees who are transferring within the Division or leaving the Division, to organize and transfer open enforcement files to another staff member and prepare their closed enforcement files for proper disposition. Each staff member shall certify their compliance with their Section's protocol and this RRG prior to their departure. Moreover, all staff members must submit the Department's Records Exit Checklist to the CRT Records Manager or designee. By completing the checklist, employees affirm that you have not removed any government material, including working files, without obtaining specific authorization for such removal from the AAG or his/her designee. *See* DOJ Policy Statement 0801.02 (Removal of and Access to Department of Justice Information, section II (Requests for Removal of Information), subsection A (Departing Employees).

**From:** Riordan, Maureen (CRT) (b)(6)
(b)(6)
**Sent:** 8/13/2025 6:08:40 PM
**To:** Gates, Michael (CRT) (b)(6) Mellett, Timothy F (CRT) (b)(6)
**Subject:** Tim, please review the redline versions. Send me any comments and then we can send to Michael. Thx
**Attachments:** Reply to CA - 2nd Demand 52 USC 20703 msr.docx; Template for State Not Yet Responding 2025 msr.docx; Template for State Providing Lists 2025 msr.docx

---

**From:** Gates, Michael (CRT) (b)(6)
**Sent:** Wednesday, August 13, 2025 1:28 PM
**To:** Riordan, Maureen (CRT) (b)(6)
**Subject:** FW: Proposed Letters

Since Jesus is out of the office and we are trying to get these done ASAP, I think we should take a crack at a (b)(5)
(b)(5) If you want to pick just one of these attached letters and let's work on (b)(5) in this one letter now, that may be more efficient. You and I can go back and forth on drafts until we both feel its ready to re-present to Jesus.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Gates, Michael (CRT)
**Sent:** Wednesday, August 13, 2025 1:25 PM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Cc:** Cumbee, Deborah (CRT) (b)(6); Riordan, Maureen (CRT) (b)(6)
**Subject:** RE: Proposed Letters

Thank you, Jesus. Inviting Maureen to comment further – (b)(5)

(b)(5)

(b)(5) We will redraft these letters and send you a second round.

(b)(5)

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**From:** Osete, Jesus (CRT) <(b)(6)>
**Sent:** Wednesday, August 13, 2025 12:14 PM
**To:** Gates, Michael (CRT) (b)(6)
**Cc:** Cumbee, Deborah (CRT) <(b)(6)>; Riordan, Maureen (CRT) <(b)(6)>
**Subject:** RE: Proposed Letters

Deborah will send you my edits/comments on MN but at a high level I think we're overcomplicating these replies.

(b)(5)

What am I missing?

**Jesus A. Osete**
Principal Deputy Assistant Attorney General
U.S. Department of Justice, Civil Rights Division

**From:** Gates, Michael (CRT) <(b)(6)>
**Sent:** Wednesday, August 13, 2025 11:02 AM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Subject:** Proposed Letters

Jesus, see attached. Once you and I finalize and approve the drafts, we can send those versions back down to our section for mass production for all states.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**From:** Gates, Michael (CRT) [(b)(6)]
**Sent:** 8/13/2025 5:27:46 PM
**To:** Riordan, Maureen (CRT) [(b)(6)]
**Subject:** FW: Proposed Letters
**Attachments:** Template for State Providing Lists 2025.docx; Template for State Not Yet Responding 2025.docx; Reply to CA - 2nd Demand 52 USC 20703.docx

Since Jesus is out of the office and we are trying to get these done ASAP, I think we should take a crack at a (b)(5) too. If you want to pick just one of these attached letters and let's work on (b)(5) in this one letter now, that may be more efficient. You and I can go back and forth on drafts until we both feel its ready to re-present to Jesus.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Gates, Michael (CRT)
**Sent:** Wednesday, August 13, 2025 1:25 PM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Cc:** Cumbee, Deborah (CRT) <(b)(6)>; Riordan, Maureen (CRT) (b)(6)
**Subject:** RE: Proposed Letters

Thank you, Jesus. Inviting Maureen to comment further – (b)(5)

(b)(5)

(b)(5) We will redraft these letters and send you a second round.

Answers to questions:

(b)(5)

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Osete, Jesus (CRT) <(b)(6)>
**Sent:** Wednesday, August 13, 2025 12:14 PM
**To:** Gates, Michael (CRT) (b)(6)
**Cc:** Cumbee, Deborah (CRT) <(b)(6)>; Riordan, Maureen (CRT) (b)(6)
**Subject:** RE: Proposed Letters

Deborah will send you my edits/comments on MN but at a high level I think we're overcomplicating these replies.

(b)(5)

What am I missing?

**Jesus A. Osete**
Principal Deputy Assistant Attorney General
U.S. Department of Justice, Civil Rights Division

---

**From:** Gates, Michael (CRT) (b)(6)
**Sent:** Wednesday, August 13, 2025 11:02 AM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Subject:** Proposed Letters

Jesus, see attached. Once you and I finalize and approve the drafts, we can send those versions back down to our section for mass production for all states.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**From:** Cumbee, Deborah (CRT) [(b)(6)]
**Sent:** 8/13/2025 7:50:04 PM
**To:** Gates, Michael (CRT) [(b)(6)]
**CC:** Riordan, Maureen (CRT) [(b)(6)]
**Subject:** RE: Proposed Letters
**Attachments:** Template for State Providing Lists 2025 (318 edits).docx; Reply to CA - 2nd Demand 52 USC 20703 (2.59 edits).docx; Template for State Not Yet Responding 2025 (325 edits).docx

No substantive edits, but attached are some redlines for punctuation.

--
Deborah Cumbee
Special Assistant, Office of Assistant Attorney General
Civil Rights Division
U.S. Department of Justice
DOJ Cell: (b)(6)

**From:** Gates, Michael (CRT) [(b)(6)]
**Sent:** Wednesday, August 13, 2025 1:25 PM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Cc:** Cumbee, Deborah (CRT) [(b)(6)]; Riordan, Maureen (CRT) [(b)(6)]
**Subject:** RE: Proposed Letters

Thank you, Jesus. Inviting Maureen to comment further – (b)(5)

(b)(5)

(b)(5) We will redraft these letters and send you a second round.

(b)(5)

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**From:** Osete, Jesus (CRT) <(b)(6)>
**Sent:** Wednesday, August 13, 2025 12:14 PM
**To:** Gates, Michael (CRT) <(b)(6)>
**Cc:** Cumbee, Deborah (CRT) <(b)(6)>; Riordan, Maureen (CRT) <(b)(6)>
**Subject:** RE: Proposed Letters

Deborah will send you my edits/comments on MN but at a high level I think we're overcomplicating these replies.

Two fundamental questions:

# (b)(5)

What am I missing?

**Jesus A. Osete**
Principal Deputy Assistant Attorney General
U.S. Department of Justice, Civil Rights Division

---

**From:** Gates, Michael (CRT) <(b)(6)
**Sent:** Wednesday, August 13, 2025 11:02 AM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Subject:** Proposed Letters

Jesus, see attached. Once you and I finalize and approve the drafts, we can send those versions back down to our section for mass production for all states.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**From**: Song, Harin C. (CRT) (b)(6)
**Sent**: 8/14/2025 2:55:11 PM
**To**: Bruzzone, Callie (CRT) (b)(6); Lott, Jasmin (CRT) (b)(6); Reid, Arielle (CRT) (b)(6); Rosenberg, Mary E. (CRT) (b)(6)
**Subject**: FW: Draft Letter for Arizona

Hi, all,

FYI I sent some questions to Tim – I was rushed in writing this and don't know if it was the best articulation of the issues but am sharing in case relevant to your letters. I welcome any thoughts. Thank you.

Best,
Harin

**From:** Song, Harin C. (CRT)
**Sent:** Thursday, August 14, 2025 10:07 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** RE: Draft Letter for Arizona

Thank you, Tim. My understanding is that the added portions are the template language paragraphs decided upon by the FO yesterday, but I have some initial questions, which I've listed below. I would like to understand the legal bases for assertions and positions reflected in this letter and other letters recently circulated, and if these issues proceed to litigation, courts may ask many of these questions. I apologize that the below may be incomplete, but I wanted to get this to you quickly. Thank you.

(b)(5)

# (b)(5)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 8:32 AM
**To:** Song, Harin C. (CRT) <(b)(6)>; Rameres, Jewel (CRT) <(b)(6)>
**Subject:** Draft Letter for Arizona

Hi Harin and Jewel,

I have attached a draft of the letter to Arizona. Let me know if you have any edits. This will need to go out this morning. Thanks,

Tim

**Sent**: 8/14/2025 3:11:30 PM
**To**: Song, Harin C. (CRT) (b)(6)
**Subject**: RE: Draft Letter for Arizona

**From:** Song, Harin C. (CRT) (b)(6)
**Sent:** Thursday, August 14, 2025 10:07 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** RE: Draft Letter for Arizona

Thank you, Tim. My understanding is that the added portions are the template language paragraphs decided upon by the FO yesterday, but I have some initial questions, which I've listed below. I would like to understand the legal bases for assertions and positions reflected in this letter and other letters recently circulated, and if these issues proceed to litigation, courts may ask many of these questions. I apologize that the below may be incomplete, but I wanted to get this to you quickly. Thank you.

(b)(5)

# (b)(5)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 8:32 AM
**To:** Song, Harin C. (CRT) <(b)(6)>; Rameres, Jewel (CRT) <(b)(6)>
**Subject:** Draft Letter for Arizona

Hi Harin and Jewel,

I have attached a draft of the letter to Arizona. Let me know if you have any edits. This will need to go out this morning. Thanks,

Tim

**From:** Gates, Michael (CRT) (b)(6)
**Sent:** 8/14/2025 2:02:18 PM
**To:** Mellett, Timothy F (CRT) (b)(6); Riordan, Maureen (CRT) (b)(6)
**Subject:** RE: (b)(5) Concerns on Letter Language

(b)(5)

Please send the letters ASAP. They will require processing and sending even after you have done what you need to do on them. That too will take time. Thank you.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 10:00 AM
**To:** Gates, Michael (CRT) (b)(6) Riordan, Maureen (CRT) (b)(6)
**Subject:** RE: (b)(5) Concerns on Letter Language

Understood. We will use the templates from last night. We won't have all 35 to you by Noon, but we will have most of them.

(b)(5)

Tim

---

**From:** Gates, Michael (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 9:31 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>; Riordan, Maureen (CRT) <(b)(6)>
**Subject:** RE: (b)(5) Concerns on Letter Language

(b)(5)

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 9:27 AM

**To:** Riordan, Maureen (CRT) <(b)(6)>
**Cc:** Gates, Michael (CRT) (b)(6)
**Subject:** RE: (b)(5) Concerns on Letter Language

I have attached the suggested revisions. Let me know if this works or if you have additional edits. Thanks,

Tim

---

**From:** Riordan, Maureen (CRT) <Maureen.Riordan2@usdoj.gov>
**Sent:** Thursday, August 14, 2025 9:01 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Cc:** Gates, Michael (CRT) <Michael.Gates2@usdoj.gov>
**Subject:** RE: (b)(5) Concerns on Letter Language

(b)(5)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 8:47 AM
**To:** Gates, Michael (CRT) <(b)(6) Riordan, Maureen (CRT) <(b)(6)>
**Cc:** Tucker, James T. (CRT) <(b)(6)>
**Subject:** (b)(5) Concerns on Letter Language

Hi Michael and Maureen,

(b)(5)

(b)(5) Let us know if we can revise the letters to make these points. If we can make these revisions, then I would also like to delete the identical footnotes. Let me know if you would like to discuss. Thanks,

Tim

---

**From:** Tucker, James T. (CRT) (b)(6)
**Sent:** Thursday, August 14, 2025 8:32 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** (b)(5) concerns

Tim,

I recommend we remove the following sentence from the letter templates:

(b)(5)

(b)(5)

Jim

**From:** Mellett, Timothy F (CRT) [(b)(6)]
**Sent:** 8/14/2025 1:27:22 PM
**To:** Riordan, Maureen (CRT) [(b)(6)]
**CC:** Gates, Michael (CRT) (b)(6)
**Subject:** RE: (b)(5) Concerns on Letter Language
**Attachments:** Template for State Providing Lists 2025 FINAL tfm.docx

I have attached the suggested revisions. Let me know if this works or if you have additional edits. Thanks,

Tim

---

**From:** Riordan, Maureen (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 9:01 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Cc:** Gates, Michael (CRT) (b)(6)
**Subject:** RE: (b)(5) Concerns on Letter Language

(b)(5)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 8:47 AM
**To:** Gates, Michael (CRT) (b)(6); Riordan, Maureen (CRT) <(b)(6)>
**Cc:** Tucker, James T. (CRT) <(b)(6)>
**Subject:** (b)(5) Concerns on Letter Language

Hi Michael and Maureen,

(b)(5)

(b)(5) Let us know if we can revise the letters to make these points. If we can make these revisions, then I would also like to delete the identical footnotes. Let me know if you would like to discuss. Thanks,

Tim

---

**From:** Tucker, James T. (CRT) <(b)(6)>
**Sent:** Thursday, August 14, 2025 8:32 AM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** (b)(5) concerns

Tim,

I recommend we remove the following sentence from the letter templates:

(b)(5)

Jim

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**From:** Gates, Michael (CRT) [(b)(6)]
**Sent:** 8/21/2025 12:54:32 PM
**To:** Osete, Jesus (CRT) [(b)(6)]
**Subject:** RE: Voter Rolls
**Attachments:** State of Michigan Final.pdf

Last PP of the letter

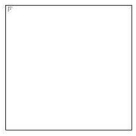
**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

---

**From:** Osete, Jesus (CRT) <(b)(6)>
**Sent:** Thursday, August 21, 2025 6:39 AM
**To:** Gates, Michael (CRT) (b)(6)
**Subject:** Re: Voter Rolls

Please send me one of the letters that describes the secure system. Thanks.

**Jesus A. Osete**
Principal Deputy Assistant Attorney General
Civil Rights Division
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20579
(b)(6)
(b)(6)



---

**From:** Gates, Michael (CRT) <(b)(6)
**Sent:** Wednesday, August 20, 2025 9:43:18 AM
**To:** Dhillon, Harmeet K. (CRT) <(b)(6)
**Cc:** Osete, Jesus (CRT) <(b)(6)>
**Subject:** Voter Rolls

When we receive the voter lists, we are going to work with states to help them into compliance. They fell asleep at the switch with DOJ not historically enforcing NVRA/HAVA. We will help them.

States will be submitting their lists to the DOJ through a secure system, which they know from our letters.

When we have their lists, we will:

(b)(5)

(b)(5)

Examples of cooperative states are Kansas, Florida, South Dakota, Virginia.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division, U.S. Department of Justice
Cell: (b)(6)

**U.S. Department of Justice**

Civil Rights Division

*Office of the Assistant Attorney General* *Washington, D.C. 20530*

August 14, 2025

Via Mail and Email

The Honorable Jocelyn Benson
Secretary of State
430 W. Allegan St.
Richard H. Austin Building – 4th Floor
Lansing, MI 48918
secretary@michigan.gov

Re: **Complete Michigan's Voter Registration List with All Fields**

Secretary Benson:

We understand that the time the Justice Department has provided your state to respond to the request for a statewide voter registration list ("VRL") and other information has not reached its deadline.

Given responses from other states thus far, we want to clarify that the Justice Department's request to provide an electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")[1] to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Michigan's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq*. Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

[1] In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

The Help America Vote Act ("HAVA"), 52 U.S.C. § 20501, *et seq*., also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq*. Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, "Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative…" 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Michigan's complete and current VRL. The purpose of the request is to ascertain Michigan's compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Michigan must ensure that it contains *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number, or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")[2] to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

> Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

HAVA specifies that the "last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974" (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained

[2] In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

in the Driver's License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency's function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

To that end, please provide the requested electronic Voter Registration List[3] to the Justice Department by the date set for your delivery by our original letter, or by August 21, 2025, whichever is later.

The information and materials may be sent by encrypted email to voting.section@usdoj.gov or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at (b)(6)

Regards,

Harmeet K. Dhillon
Assistant Attorney General
Civil Rights Division

cc: Jonathan Brater
Director, Bureau of Elections
430 W. Allegan St.
Richard H. Austin Building – 4th Floor
Lansing, MI 48918
(b)(6)

[3] Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.

**From:** Kagle, Kilian (CRT) [(b)(6)]
**Sent:** 8/27/2025 7:29:35 PM
**To:** Mellett, Timothy F (CRT) [(b)(6)]; Okwesa, Carolyn (CRT) (b)(6)
**CC:** Bryce, Amanda (CRT) [(b)(6)]
**Subject:** Re: Voting Section -- Privacy Act Questions

Since any agreement with states would not impinge on FOIA/PA obligations, those aren't routed through this Branch regrettably. We've lost our SPL PoC , so I'm at a bit of a loss on whom to direct you to, Tim.

Get Outlook for iOS

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Wednesday, August 27, 2025 2:09:30 PM
**To:** Kagle, Kilian (CRT) <(b)(6)>; Okwesa, Carolyn (CRT) (b)(6)
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** RE: Voting Section -- Privacy Act Questions

Thanks!
Do we have a sense if a statewide agreement would look the same as an interagency agreement. Have we had any data sharing agreements with other jurisdictions? I am thinking maybe Special Lit. and the police cases?

---

**From:** Kagle, Kilian (CRT) (b)(6)
**Sent:** Wednesday, August 27, 2025 1:30 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>; Okwesa, Carolyn (CRT) (b)(6)
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** RE: Voting Section -- Privacy Act Questions

I have only guidance on inter-agency data sharing but nothing with States, Tim.

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Wednesday, August 27, 2025 1:16 PM
**To:** Kagle, Kilian (CRT) <(b)(6)>; Okwesa, Carolyn (CRT) (b)(6)
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** RE: Voting Section -- Privacy Act Questions

All,

We just had a meeting with the Front Office, and they have come around to the idea of having a data sharing agreement with states who will send us the Drivers License numbers and last 4 of SSN. Do you have a template? The idea would be to include the data sharing agreement template with the letter answering the questions about the SORN, etc. Thanks,

Tim

---

**From:** Kagle, Kilian (CRT) <(b)(6)>
**Sent:** Wednesday, August 27, 2025 10:38 AM
**To:** Okwesa, Carolyn (CRT) (b)(6) Mellett, Timothy F (CRT) <(b)(6)>
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** RE: Voting Section -- Privacy Act Questions

Absolutely, Carolyn. The FR citations are 68 FR 47610, 611 (8-11-2003), 70 FR 43904 (7-29-2005), 82 FR 24147 (5-25-2017). For questions 2 & 3, I recommend reciting the exact language in SORN CRT-001. (attached hereto).

---

**From:** Okwesa, Carolyn (CRT) (b)(6)
**Sent:** Wednesday, August 27, 2025 9:30 AM
**To:** Kagle, Kilian (CRT) <(b)(6)>
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** FW: Voting Section -- Privacy Act Questions

Good morning Kilian,
Voting is looking for guidance on a response they plan to send out today. (See email below.)
Could you speak with Tim regarding the questions he has listed below?
Thank you,
Carolyn

**Carolyn Okwesa**
**Project Manager (Contractor) | Office of Information Technology and Cybersecurity**
**U.S. Department of Justice | Civil Rights Division | Administrative Management Section**
(b)(6)
(b)(6)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Tuesday, August 26, 2025 5:35 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for looking at this. I think we were hoping to get a letter out later this week.
Yes, tomorrow afternoon would be fine to meet. Brittany Wake and Nadine Jones also should be invited.

Tim

---

**From:** Bryce, Amanda (CRT) (b)(6)
**Sent:** Tuesday, August 26, 2025 4:59 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Tim,

I hope to have some follow-up response to you by next week. In the meantime, could we chat tomorrow about the discontinuance of FOIA express ? If there is time, also discuss STAPS.

Let me know if I could schedule it for tomorrow and who to invite.

Amanda Bryce
Chief Information Officer
U.S. Department of Justice | Civil Rights Division
(b)(6)
(b)(6)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Monday, August 25, 2025 6:19 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for discussing the Privacy Act/data sharing questions the other week. We have requested voter registration lists from states to conduct searches that assess the List Maintenance of voter registration lists under the National Voter Registration Act and the Help America Vote Act (statutes that the Voting Section enforces). Some states have asked us a few Privacy Act questions because the data contains PII. At the moment, we are looking to write a letter to states that have asked the following questions:

1. Please provide a citation within the Federal Register to the system of records under which DOJ intends to collect and maintain the records it has requested.
   (We are thinking that it would be CRT-1, but we wanted to be sure, and we did not know if there would be others).
2. Please describe how DOJ plans to store, maintain, and use the requested voter registration information.
   (We can answer the "use" question but we don't know what we should say about store and maintain. Lit Support has this on the P Drive.)
3. Please explain who will have access to the information contained in the Voter Registration List.
   (Lit Support has permissions limited to managers and those attorneys and analysts working on the matters. I did not know how big of scope there could be while complying with the Privacy Act. Voting only? CRT only? DOJ only?)

Ideally, we would like to send the letters out on Wednesday. Happy to chat if you have questions. Thanks,

Tim Mellett
Deputy Chief, Voting Section
(b)(6)

**From:** Kagle, Kilian (CRT) [redacted]
**Sent:** 8/27/2025 5:29:58 PM
**To:** Mellett, Timothy F (CRT) [redacted] Okwesa, Carolyn (CRT) [redacted]
**CC:** Bryce, Amanda (CRT) [redacted]
**Subject:** RE: Voting Section -- Privacy Act Questions
**Attachments:** sampleinteragencydatasharingagreement.doc; OMB_M-11-02 Data Sharing.pdf; OMB_M-01-05 Data Sharing.pdf

I have only guidance on inter-agency data sharing but nothing with States, Tim.

---

**From:** Mellett, Timothy F (CRT) <[redacted]>
**Sent:** Wednesday, August 27, 2025 1:16 PM
**To:** Kagle, Kilian (CRT) <[redacted]>; Okwesa, Carolyn (CRT) [redacted]
**Cc:** Bryce, Amanda (CRT) <[redacted]>
**Subject:** RE: Voting Section -- Privacy Act Questions

All,

We just had a meeting with the Front Office, and they have come around to the idea of having a data sharing agreement with states who will send us the Drivers License numbers and last 4 of SSN. Do you have a template? The idea would be to include the data sharing agreement template with the letter answering the questions about the SORN, etc. Thanks,

Tim

---

**From:** Kagle, Kilian (CRT) <[redacted]>
**Sent:** Wednesday, August 27, 2025 10:38 AM
**To:** Okwesa, Carolyn (CRT) [redacted] Mellett, Timothy F (CRT) <[redacted]>
**Cc:** Bryce, Amanda (CRT) <[redacted]>
**Subject:** RE: Voting Section -- Privacy Act Questions

Absolutely, Carolyn. The FR citations are 68 FR 47610, 611 (8-11-2003), 70 FR 43904 (7-29-2005), 82 FR 24147 (5-25-2017). For questions 2 & 3, I recommend reciting the exact language in SORN CRT-001. (attached hereto).

---

**From:** Okwesa, Carolyn (CRT) <[redacted]>
**Sent:** Wednesday, August 27, 2025 9:30 AM
**To:** Kagle, Kilian (CRT) <[redacted]>
**Cc:** Bryce, Amanda (CRT) <[redacted]>
**Subject:** FW: Voting Section -- Privacy Act Questions

Good morning Kilian,
Voting is looking for guidance on a response they plan to send out today. (See email below.)
Could you speak with Tim regarding the questions he has listed below?
Thank you,
Carolyn

**Carolyn Okwesa**
**Project Manager (Contractor) | Office of Information Technology and Cybersecurity**

U.S. Department of Justice | Civil Rights Division | Administrative Management Section
(b)(6)
(b)(6)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Tuesday, August 26, 2025 5:35 PM
**To:** Bryce, Amanda (CRT) <(b)(6)>
**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for looking at this. I think we were hoping to get a letter out later this week.
Yes, tomorrow afternoon would be fine to meet. Brittany Wake and Nadine Jones also should be invited.

Tim

**From:** Bryce, Amanda (CRT) (b)(6)
**Sent:** Tuesday, August 26, 2025 4:59 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>
**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Tim,

I hope to have some follow-up response to you by next week. In the meantime, could we chat tomorrow about the discontinuance of FOIA express ? If there is time, also discuss STAPS.

Let me know if I could schedule it for tomorrow and who to invite.

Amanda Bryce
Chief Information Officer
U.S. Department of Justice | Civil Rights Division
(b)(6)
(b)(6)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Monday, August 25, 2025 6:19 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for discussing the Privacy Act/data sharing questions the other week. We have requested voter registration lists from states to conduct searches that assess the List Maintenance of voter registration lists under the National Voter Registration Act and the Help America Vote Act (statutes that the Voting Section enforces). Some states have asked us a

few Privacy Act questions because the data contains PII. At the moment, we are looking to write a letter to states that have asked the following questions:

1. Please provide a citation within the Federal Register to the system of records under which DOJ intends to collect and maintain the records it has requested.
   (We are thinking that it would be CRT-1, but we wanted to be sure, and we did not know if there would be others).
2. Please describe how DOJ plans to store, maintain, and use the requested voter registration information.
   (We can answer the "use" question but we don't know what we should say about store and maintain. Lit Support has this on the P Drive.)
3. Please explain who will have access to the information contained in the Voter Registration List.
   (Lit Support has permissions limited to managers and those attorneys and analysts working on the matters. I did not know how big of scope there could be while complying with the Privacy Act. Voting only? CRT only? DOJ only?)

Ideally, we would like to send the letters out on Wednesday. Happy to chat if you have questions. Thanks,

Tim Mellett
Deputy Chief, Voting Section
(b)(6)

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

November 3, 2010

M-11-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jeffrey D. Zients
Deputy Director for Management

Cass R. Sunstein
Administrator, Office of Information and Regulatory Affairs

SUBJECT: Sharing Data While Protecting Privacy

The judicious use of accurate and reliable data plays a critical role in initiatives designed to increase the transparency and efficiency of Federal programs and to enhance our capacity to gauge program effectiveness. Sharing data among agencies also allows us to achieve better outcomes for the American public through more accurate evaluation of policy options, improved stewardship of taxpayer dollars, reduced paperwork burdens, and more coordinated delivery of public services.

As advances in technology enhance tools for data sharing, Federal agencies can and should seek new approaches for identifying and sharing high-value data responsibly and appropriately. This Memorandum strongly encourages Federal agencies to engage in coordinated efforts to share high-value data for purposes of supporting important Administration initiatives, informing public policy decisions, and improving program implementation while simultaneously embracing responsible stewardship.

When agencies share data, they must do so in a way that fully protects individual privacy. The public must be able to trust our ability to handle and protect personally identifiable information.[1] In sharing data, agencies must comply with the Privacy Act of 1974[2] and all other applicable privacy laws, regulations, and policies. In addition to the legal framework that governs the use and disclosure of data, agencies are advised to consult established codes of Fair Information Practices.[3] As OMB has previously noted, "[t]he individual's right to privacy must

[1] For the definition of "personally identifiable information," see the appendix to OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

[2] 5 U.S.C. § 552a.

[3] Since 1973, several government reports – both general and agency-specific – have established Fair Information Practices that set forth many accepted principles of information privacy. *See, e.g.*, U.S. Dep't of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the*

be protected in Federal Government information activities involving personal information."[4]

Data sharing is critical to successful initiatives in many domains. The purpose of this Memorandum is to direct agencies to find solutions that allow data sharing to move forward in a manner that complies with applicable privacy laws, regulations, and polices. These collaborative efforts should include seeking ways to facilitate responsible data sharing for the purpose of conducting rigorous studies that promote informed public policy decisions.

***Benefits of Sharing***. Greater sharing of data can help the Federal Government serve the public with programs that reflect the highest degree of efficiency, coordination, and accountability. Some of the potential benefits of data sharing include:

- Timely and improved access to reliable and high-quality data to inform decision-making by the Administration as well as Congress.

- Increased transparency, better service, and reduced risk of waste, fraud, and abuse with respect to public programs.

- More informed research on public policy as a result of an increased number of theoretical and empirical studies that rigorously analyze, and augment the understanding of, Federal programs within government for the public at large.

- Improved government efficiency and reduced paperwork burdens as a result of more informed decision-making and a reduction in burdensome, excessive, and duplicative data-collection activities.

***Important Initiatives***. The success of many initiatives hinges on the sharing of high-value data. Examples of how data sharing could play a significant role in important initiatives include:

- Do Not Pay List: Our ability to eliminate improper payments, such as those to fraudulent vendors or to deceased individuals, could benefit from information about payee status.

- Evaluation Initiative: Our ability to measure the success of programs – from education and job training to health care management – would improve with access to administrative data for evaluation and evidence-building.

- Statistics Initiative: Our ability to contain costs and reduce burdens on respondents, while increasing the quality and quantity of statistical information, depends on the untapped potential of data sets held by program, administrative, and regulatory offices and agencies.

---

*Rights of Citizens* (1973), available at http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[4] OMB Circular A-130, *Management of Federal Information Resources*, available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

- Partnership Fund for Program Integrity Innovation: Our ability to identify, implement, and test methods to improve integrity, efficiency, and service in the delivery of State and Federal benefit programs will increase with more information about eligibility and enrollment status across programs and levels of government.

Federal agencies are encouraged to engage in coordinated efforts to share high-value data for purposes of supporting important Administration initiatives, informing public policy decisions, and improving program implementation. These efforts should include:

(1) identifying high-value data that would promote effective and efficient decision-making;

(2) identifying high-value data and data sharing methodologies that would promote more efficient delivery of Federal, State, and local benefits with lower error rates;

(3) developing effective approaches for properly sharing data with other Federal entities, consistent with applicable laws, regulations, and policies;

(4) ensuring the use of common data standards (e.g., NIEM, XBRL, XML) to promote greater interoperability across systems and improving sharing of data as part of IT modernization initiatives; and

(5) following Enterprise Architecture guidance and principles consistent with appropriate OMB guidance and best practices for new and on-going systems development and implementation.

Sharing data in external public policy, scientific, and other areas of research is of value to the public and can promote savings. In cases where high-value data contain information that is protected under Federal privacy laws, agencies are encouraged, to the extent permitted by law, to develop and implement arrangements that would permit access to these data for research purposes subject to the appropriate safeguards.

***Compliance with Privacy Laws, Regulations, and Policies***. Whenever Federal agencies carry out data sharing activities, including pursuant to this Memorandum, all participants must comply with applicable privacy laws, regulations, and policies.

It is also important to recognize that, whereas the Privacy Act of 1974 imposes generally applicable prohibitions and requirements regarding information about individuals that is contained in systems of records, other statutes provide privacy protections with respect to particular categories of information. The nature of these privacy protections differs under the various statutes. For example, laws may distinguish between (1) interagency sharing of personally identifiable information in ways that generate only aggregate statistical results and (2) uses of data that involve public disclosure of personally identifiable information. In addition, agencies that are either sharing or receiving data must determine whether, under applicable laws, regulations, and policies, the prohibitions and requirements that apply to particular data will continue to apply after data are shared with an agency or other recipient. Federal agencies

should consult applicable OMB guidance pertaining to privacy laws, regulations, and policies when considering data sharing activities.[5]

Moreover, nothing in this Memorandum shall be construed to promote or favor data sharing that could threaten national security, breach confidentiality, or damage other genuinely compelling interests. OMB stands ready to assist agencies as they evaluate proposals for data sharing activities and as they take the necessary steps for ensuring that their data sharing activities comply with applicable laws, regulations, and policies.

Pursuant to this Memorandum, OMB may ask specific agencies to perform an evaluation and submit a written report detailing options for authorized data sharing; if so, OMB will be available to address relevant questions. The report should be signed by an agency's Senior Agency Official for Privacy, and it should identify any steps that must be taken before data sharing may occur.

***Queries***. Agencies with questions about this Memorandum or about ways to improve government performance through the sharing of data may contact OMB at datause@omb.eop.gov. OMB will draw on expertise across the agency, including its privacy experts, in formulating its response.

[5] *See, e.g.*, *Privacy Act Implementation*, 40 Fed. Reg. 28,948-78 (July 9, 1975); *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988*, 54 Fed. Reg. 25,818-29 (June 16, 1989). All OMB privacy guidance is available at http://www.whitehouse.gov/omb/inforeg_infopoltech#pg.

December 20, 2000

**M-01-05**

**MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES**

FROM: Jacob J. Lew
Director

SUBJECT:Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy

OMB is issuing guidance to remind agencies of several privacy-related legal requirements that apply to computer matching and to clarify how agencies should conduct computer matching activities. This guidance applies to data matching activities or programs for purposes of establishing or verifying eligibility for Federal benefit programs or recouping payments or delinquent debts under such programs covered by the Computer Matching and Privacy Protection Act ("Matching Act"),[(1)] an amendment to the Privacy Act of 1974, 5 U.S.C. Section 552a, whether data are shared between Federal agencies or matched with State agency data.[(2)] Although this guidance applies directly only to programs covered by the Matching Act, agencies should consider applying these principles in other data sharing contexts.

Inter-agency sharing of information about individuals can be an important tool in improving the efficiency of government programs. By sharing data, agencies can often reduce errors, improve program efficiency, identify and prevent fraud, find intended beneficiaries, evaluate program performance, and reduce information collection burden on the public.

As government increasingly moves to electronic collection and dissemination of data, under the Government Paperwork Elimination Act and other programs, opportunities to share data across agencies will likely increase. Agencies should work together to determine what data sharing opportunities are desirable, feasible, and appropriate. In general, data sharing should only be pursued if the benefits outweigh the costs.

With increased focus on data sharing, agencies must pay close attention to handling responsibly their own data and the data they share with or receive from other agencies. When information about individuals is involved, agencies must pay especially close attention to privacy interests and must incorporate measures to safeguard those interests. Prior to any data sharing, agencies must review and meet the Privacy Act requirements for computer matching, including developing a computer matching agreement and publishing notice of the proposed match in the *Federal Register*; OMB Guidance on Computer Matching (54 *Fed. Reg.* 25818, June 19, 1989); and OMB Circular A-130, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals." Agencies must also review and meet applicable requirements under other laws, including the Paperwork Reduction Act of 1995.

The attached memorandum puts forth principles on protecting personal privacy when conducting inter-agency data sharing. Agencies themselves, as well as inter-agency work groups, such as the

Chief Financial Officers (CFO) Council, the Chief Information Officers (CIO) Council, the President's Council on Integrity and Efficiency, the Procurement Executives Council (PEC), and the Human Resources Management Council (HRMC) should ensure that they adhere to the principles.

For any questions about this guidance, contact Lauren Steinfeld or Brooke Dickson of the Office of Information and Regulatory Affairs, Office of Management and Budget. Lauren Steinfeld can be reached at phone (202) 395-3647, fax (202) 395-3047, e-mail Lauren_Steinfeld@omb.eop.gov. Brooke Dickson can be reached at phone (202) 395-3191, fax (202) 395-5167, e-mail Brooke_Dickson@omb.eop.gov.

Attachment

---

## ATTACHMENT

## Privacy Principles in Conducting Inter-Agency Data Sharing

## Existing Requirements

1. **Notice.**
   Agencies that plan to use data sharing to verify program eligibility or to recover delinquent debt should develop procedures for providing notice to the individual at the time of application, and periodically thereafter (as directed by the Data Integrity Board), that the information they provide may be subject to verification through matching programs, as required by the Matching Act. In addition to direct notice to individuals, the Matching Act requires that agencies publish a notice in the Federal Register, at least 30 days before conducting the data match, describing the purpose of the match, the records and individuals covered, and other relevant information.

2. **Consent, As Appropriate.**

   Agencies should obtain the written (or electronic) consent of individuals before sharing personal data protected by the Privacy Act, unless one of the exceptions under Section 552a(b) of the Privacy Act applies.

3. **Redisclosure Limitations.**

   Data sharing programs should prohibit the redisclosure of the data, except as allowed under the Matching Act. Specifically, the Matching Act prohibits recipient agencies, whether Federal or State, from redisclosing records, except where required by law or where the redisclosure is essential to the conduct of the matching program.

4. **Accuracy.**

   Because information shared among agencies may be used to deny, reduce, or otherwise adversely affect benefits to individuals, it is critical that agencies have reasonable procedures to ensure the accuracy of the data shared. At a minimum, this should include providing individuals the right to access and to request amendment of their records, as required by the Privacy Act.

   To ensure accuracy, agencies must also adhere to the due process requirements found in the Matching Act. Pursuant to 5 U.S.C. 552a(p), before an agency takes adverse action against an individual based on the results of information produced by a matching program, it must independently verify the information unless there is a determination by the relevant Data Integrity Board, for a limited class of information, that there is a high degree of confidence that the information is accurate. Agencies must also, at least 30 days before taking adverse action (unless statute or regulation states otherwise), provide notice to the individual of the agency's findings and provide an opportunity to contest those

findings. These requirements do not apply in situations where public health or public safety may be adversely affected or significantly threatened.

5. **Security Controls.**

Agencies should employ adequate and effective security controls to protect the confidentiality, availability, and integrity of all systems and data, including all data shared with other organizations. Agencies should ensure, prior to the sharing of any data, that the recipient organization affords the appropriate equivalent level of security controls as maintained by the originating agency. Since data security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization.

Both originating and recipient agencies should consider and apply all appropriate management, operational, and technical security controls commensurate with the level of risk and magnitude of harm that would occur if the security of the data and the systems that process it were breached. Agencies should particularly consider physical security needs, such as whether personal information is so sensitive that it should be kept in an approved security container, or whether access to where the information is located should be limited. Agencies should also consider personnel security needs, such as additional controls over individuals who have access to data. They should also consider network security, including encryption for data in transit and protection for data at rest. In addition, agencies receiving data via data sharing must have procedures for the retention and timely destruction of identifiable records. Especially for more sensitive data, audit trails and other anti-browsing features may be appropriate in the recipient agency. For further guidance on ensuring adequate security, *see* OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" and all associated National Institute of Standards and Technology (NIST) computer security guidance.

**Additional Guidance**

6. **Minimization.**

When dealing with paper records, it may be difficult to provide only certain data elements to other agencies, because of the need for manual redaction of other information. In the computer world, it is far easier to implement sharing of only a narrow range of information that is necessary to verify an applicant's eligibility for a program. Agencies should analyze what data are needed for program purposes and make every effort to ensure that they transfer only that information.

7. **Accountability.**

Data sharing programs should include mechanisms to ensure that agencies are accountable for adhering to these principles. Some of these measures are already found in the Privacy Act, which provides for civil and criminal penalties for non-compliance.

Agencies should also consider training programs that stress accountability and explain penalties for breaches of confidentiality. Especially for more sensitive data and more extensive data sharing arrangements, agencies should consider whether additional oversight mechanisms, such as self-audits, are justified.

For example, agencies should establish procedures to ensure compliance with redisclosure limitations. One mechanism for assuring compliance would be to have the recipient agency certify on a periodic basis that it has examined practices regarding redisclosure and, if necessary, taken corrective action where improper redisclosures have occurred.

8. **Privacy Impact Assessments.**

In the President's FY2001 budget, the President announced an initiative to make "privacy impact assessments," or "PIAs," a regular part of the development of new Government computer systems. A PIA is a plan to build privacy protection into new information systems, such as, for example, by asking systems personnel and program personnel to work through questions on data needs and data protection *before* the system is developed. The CIO Council has voted the IRS PIA a best practice; it is available as a reference at http://www.cio.gov.

For any questions about this guidance, contact Lauren Steinfeld or Brooke Dickson of the Office of Information and Regulatory Affairs, Office of Management and Budget. Lauren Steinfeld can be reached at phone (202) 395-3647, fax (202) 395-3047, e-mail Lauren_Steinfeld@omb.eop.gov. Brooke Dickson can be reached at phone (202) 395-3191, fax (202) 395-5167, e-mail Brooke_Dickson@omb.eop.gov.

---

1. For purposes of this guidance, "data sharing" means data matching activities or programs covered under the Computer Matching and Privacy Protection Act.

2. This guidance does not apply to several types of matching activities or programs excluded by the Matching Act, such as matches performed to produce aggregate statistical data without any personal identifiers and matches performed to support any research or statistical project. Such data may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals.

**From:** Bryce, Amanda (CRT) [A (b)(6) ]
**Sent:** 8/27/2025 3:15:09 PM
**To:** Kagle, Kilian (CRT) [ (b)(6) ]
**Subject:** RE: Voting Section -- Privacy Act Questions

I see. Were they advised in writing, if so can you share it w/ me?

Thanks.

---

**From:** Kagle, Kilian (CRT) < (b)(6) >
**Sent:** Wednesday, August 27, 2025 10:51 AM
**To:** Bryce, Amanda (CRT) < (b)(6) >
**Subject:** RE: Voting Section -- Privacy Act Questions

Hopefully, they are all set with my answer to Carolyn. Reciting the SORN is the extent to which I

(b)(5)

---

**From:** Bryce, Amanda (CRT) (b)(6)
**Sent:** Wednesday, August 27, 2025 10:46 AM
**To:** Kagle, Kilian (CRT) < (b)(6) >
**Subject:** RE: Voting Section -- Privacy Act Questions

Kilian,

Looks like they are wanting to have something drafted today.

---

**From:** Kagle, Kilian (CRT) < (b)(6) >
**Sent:** Wednesday, August 27, 2025 10:24 AM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Good morning, Amanda. Thank you, I'll try to nudge VOT in the right direction.

---

**From:** Bryce, Amanda (CRT) (b)(6)
**Sent:** Tuesday, August 26, 2025 4:58 PM
**To:** Kagle, Kilian (CRT) < (b)(6) >
**Cc:** Cononie, Sean (CRT) < (b)(6) >
**Subject:** FW: Voting Section -- Privacy Act Questions

Could we meet on Friday and talk this over?

Amanda Bryce
Chief Information Officer
U.S. Department of Justice | Civil Rights Division
(b)(6)
(b)(6)

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Monday, August 25, 2025 6:19 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for discussing the Privacy Act/data sharing questions the other week. We have requested voter registration lists from states to conduct searches that assess the List Maintenance of voter registration lists under the National Voter Registration Act and the Help America Vote Act (statutes that the Voting Section enforces). Some states have asked us a few Privacy Act questions because the data contains PII. At the moment, we are looking to write a letter to states that have asked the following questions:

1. Please provide a citation within the Federal Register to the system of records under which DOJ intends to collect and maintain the records it has requested.
   (We are thinking that it would be CRT-1, but we wanted to be sure, and we did not know if there would be others).
2. Please describe how DOJ plans to store, maintain, and use the requested voter registration information.
   (We can answer the "use" question but we don't know what we should say about store and maintain. Lit Support has this on the P Drive.)
3. Please explain who will have access to the information contained in the Voter Registration List.
   (Lit Support has permissions limited to managers and those attorneys and analysts working on the matters. I did not know how big of scope there could be while complying with the Privacy Act. Voting only? CRT only? DOJ only?)

Ideally, we would like to send the letters out on Wednesday. Happy to chat if you have questions. Thanks,

Tim Mellett
Deputy Chief, Voting Section
(b)(6)

**From:** Mellett, Timothy F (CRT) [(b)(6)]
**Sent:** 8/27/2025 3:05:56 PM
**To:** Kagle, Kilian (CRT) [(b)(6)]; Okwesa, Carolyn (CRT) [(b)(6)]
**CC:** Bryce, Amanda (CRT) [(b)(6)]
**Subject:** RE: Voting Section -- Privacy Act Questions

Thanks!

---

**From:** Kagle, Kilian (CRT) [(b)(6)]
**Sent:** Wednesday, August 27, 2025 10:38 AM
**To:** Okwesa, Carolyn (CRT) [(b)(6)]; Mellett, Timothy F (CRT) <[(b)(6)]>
**Cc:** Bryce, Amanda (CRT) <[(b)(6)]>
**Subject:** RE: Voting Section -- Privacy Act Questions

Absolutely, Carolyn. The FR citations are 68 FR 47610, 611 (8-11-2003), 70 FR 43904 (7-29-2005), 82 FR 24147 (5-25-2017). For questions 2 & 3, I recommend reciting the exact language in SORN CRT-001. (attached hereto).

---

**From:** Okwesa, Carolyn (CRT) [(b)(6)]
**Sent:** Wednesday, August 27, 2025 9:30 AM
**To:** Kagle, Kilian (CRT) <[(b)(6)]>
**Cc:** Bryce, Amanda (CRT) <[(b)(6)]>
**Subject:** FW: Voting Section -- Privacy Act Questions

Good morning Kilian,
Voting is looking for guidance on a response they plan to send out today. (See email below.)
Could you speak with Tim regarding the questions he has listed below?
Thank you,
Carolyn

**Carolyn Okwesa**
**Project Manager (Contractor) | Office of Information Technology and Cybersecurity**
**U.S. Department of Justice | Civil Rights Division | Administrative Management Section**
[(b)(6)]
[(b)(6)]

---

**From:** Mellett, Timothy F (CRT) <[(b)(6)]>
**Sent:** Tuesday, August 26, 2025 5:35 PM
**To:** Bryce, Amanda (CRT) [(b)(6)]
**Cc:** Okwesa, Carolyn (CRT) [(b)(6)]
**Subject:** RE: Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for looking at this. I think we were hoping to get a letter out later this week.
Yes, tomorrow afternoon would be fine to meet. Brittany Wake and Nadine Jones also should be invited.

Tim

---

**From:** Bryce, Amanda (CRT) (b)(6)
**Sent:** Tuesday, August 26, 2025 4:59 PM
**To:** Mellett, Timothy F (CRT) (b)(6)
**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Tim,

I hope to have some follow-up response to you by next week. In the meantime, could we chat tomorrow about the discontinuance of FOIA express ? If there is time, also discuss STAPS.

Let me know if I could schedule it for tomorrow and who to invite.

Amanda Bryce
Chief Information Officer
U.S. Department of Justice | Civil Rights Division
(b)(6)
(b)(6)

---

**From:** Mellett, Timothy F (CRT) (b)(6)
**Sent:** Monday, August 25, 2025 6:19 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for discussing the Privacy Act/data sharing questions the other week. We have requested voter registration lists from states to conduct searches that assess the List Maintenance of voter registration lists under the National Voter Registration Act and the Help America Vote Act (statutes that the Voting Section enforces). Some states have asked us a few Privacy Act questions because the data contains PII. At the moment, we are looking to write a letter to states that have asked the following questions:

1. Please provide a citation within the Federal Register to the system of records under which DOJ intends to collect and maintain the records it has requested.
   (We are thinking that it would be CRT-1, but we wanted to be sure, and we did not know if there would be others).
2. Please describe how DOJ plans to store, maintain, and use the requested voter registration information.
   (We can answer the "use" question but we don't know what we should say about store and maintain. Lit Support has this on the P Drive.)
3. Please explain who will have access to the information contained in the Voter Registration List.
   (Lit Support has permissions limited to managers and those attorneys and analysts working on the matters. I did not know how big of scope there could be while complying with the Privacy Act. Voting only? CRT only? DOJ only?)

Ideally, we would like to send the letters out on Wednesday. Happy to chat if you have questions. Thanks,

Tim Mellett
Deputy Chief, Voting Section
(b)(6)

**From:** Kagle, Kilian (CRT) [(b)(6)
(b)(6)]
**Sent:** 8/27/2025 2:38:14 PM
**To:** Okwesa, Carolyn (CRT) [(b)(6)]; Mellett, Timothy F (CRT) [(b)(6)]
**CC:** Bryce, Amanda (CRT) [(b)(6)]
**Subject:** RE: Voting Section -- Privacy Act Questions
**Attachments:** 03-20342.pdf

Absolutely, Carolyn. The FR citations are 68 FR 47610, 611 (8-11-2003), 70 FR 43904 (7-29-2005), 82 FR 24147 (5-25-2017). For questions 2 & 3, I recommend reciting the exact language in SORN CRT-001. (attached hereto).

---

**From:** Okwesa, Carolyn (CRT) <(b)(6)>
**Sent:** Wednesday, August 27, 2025 9:30 AM
**To:** Kagle, Kilian (CRT) <(b)(6)>
**Cc:** Bryce, Amanda (CRT) <(b)(6)>
**Subject:** FW: Voting Section -- Privacy Act Questions

Good morning Kilian,
Voting is looking for guidance on a response they plan to send out today. (See email below.)
Could you speak with Tim regarding the questions he has listed below?
Thank you,
Carolyn

**Carolyn Okwesa**
**Project Manager (Contractor) | Office of Information Technology and Cybersecurity**
**U.S. Department of Justice | Civil Rights Division | Administrative Management Section**
(b)(6)
(b)(6)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Tuesday, August 26, 2025 5:35 PM
**To:** Bryce, Amanda (CRT) <(b)(6)>
**Cc:** Okwesa, Carolyn (CRT) <(b)(6)>
**Subject:** RE: Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for looking at this. I think we were hoping to get a letter out later this week.
Yes, tomorrow afternoon would be fine to meet. Brittany Wake and Nadine Jones also should be invited.

Tim

---

**From:** Bryce, Amanda (CRT) <(b)(6)>
**Sent:** Tuesday, August 26, 2025 4:59 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>

**Cc:** Okwesa, Carolyn (CRT) (b)(6)
**Subject:** RE: Voting Section -- Privacy Act Questions

Tim,

I hope to have some follow-up response to you by next week. In the meantime, could we chat tomorrow about the discontinuance of FOIA express ? If there is time, also discuss STAPS.

Let me know if I could schedule it for tomorrow and who to invite.

Amanda Bryce
Chief Information Officer
U.S. Department of Justice | Civil Rights Division
(b)(6)
(b)(6)

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Monday, August 25, 2025 6:19 PM
**To:** Bryce, Amanda (CRT) (b)(6)
**Subject:** Voting Section -- Privacy Act Questions

Hi Amanda,

Thanks for discussing the Privacy Act/data sharing questions the other week. We have requested voter registration lists from states to conduct searches that assess the List Maintenance of voter registration lists under the National Voter Registration Act and the Help America Vote Act (statutes that the Voting Section enforces). Some states have asked us a few Privacy Act questions because the data contains PII. At the moment, we are looking to write a letter to states that have asked the following questions:

1. Please provide a citation within the Federal Register to the system of records under which DOJ intends to collect and maintain the records it has requested.
   (We are thinking that it would be CRT-1, but we wanted to be sure, and we did not know if there would be others).
2. Please describe how DOJ plans to store, maintain, and use the requested voter registration information.
   (We can answer the "use" question but we don't know what we should say about store and maintain. Lit Support has this on the P Drive.)
3. Please explain who will have access to the information contained in the Voter Registration List.
   (Lit Support has permissions limited to managers and those attorneys and analysts working on the matters. I did not know how big of scope there could be while complying with the Privacy Act. Voting only? CRT only? DOJ only?)

Ideally, we would like to send the letters out on Wednesday. Happy to chat if you have questions. Thanks,

Tim Mellett
Deputy Chief, Voting Section
(b)(6)

**SUPPLEMENTARY INFORMATION:** The Commission instituted this investigation on January 24, 2003, based on a complaint filed by Charles D. Walkden (''Walkden'') of Homer, Alaska. 68 FR 3550 (2003). The complaint, as amended, alleged violations of section 337 in the importation, sale for importation, and sale within the United States after importation of certain truck bed ramps and components thereof that infringe claim 1 of U.S. Patent No. 5,795,125 (''the '125 patent''). The Commission named as respondents ETEC of Saskatoon, SK, Canada; Textron Inc. (''Textron'') of Providence, Rhode Island; VIP Distributing of Anchorage, Alaska; Southwest Distributing Co. of Clinton, Oklahoma; and Hamilton Equipment Inc. of Ephrata, Pennsylvania. *Id.* Textron was subsequently terminated from the investigation on the basis of a consent order.

On June 2, 2003, the Commission investigative attorney (''IA'') moved pursuant to Commission rule 210.15(a) for summary determination of non-infringement. On July 10, 2003, the ALJ issued an ID granting the IA's motion. No petitions for review of the ID were filed.

This action is taken under the authority of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. 1337), and 210.42 of the Commission's Rules of Practice and Procedure (19 CFR 210.42).

Issued: August 6, 2003.

By order of the Commission.

**Marilyn R. Abbott,**

*Secretary to the Commission.*

[FR Doc. 03–20384 Filed 8–8–03; 8:45 am]

**BILLING CODE 7020–02–P**

## DEPARTMENT OF JUSTICE

**[AAG/A Order No. 015–2003]**

### Privacy Act of 1974; Systems of Records

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), the Department proposes to modify the following Privacy Act systems of records:

Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT–001 (previously published on February 20, 1998, at 63 FR 8659);

Civil Rights Case Load Evaluation System—Time Reporting System, JUSTICE/CRT–003 (previously published on October 17, 1988, at 53 FR 40510);

Registry of Names of Interested Persons Desiring Notifications of Submissions Under Section 5 of the Voting Rights Act, JUSTICE/CRT–004 (previously published on October 17, 1988, at 53 FR 40511);

Files on Employment Civil Rights Matters from Persons Outside of the Department of Justice, JUSTICE/CRT–007 (previously published on October 17, 1988, at 53 FR 40512); and Civil Rights Division Travel Reports, JUSTICE/CRT–009 (previously published on October 17, 1988, at 53 FR 40514).

The Department is publishing modifications to the above systems of records. This notice includes some major changes such as adding new routine uses. Also, the Department made other non-substantive changes in all the above systems to provide clarification, such as to correct typographical errors, to provide updated addresses, to update information on particular statutes, to clarify existing routine uses, to add data elements omitted from previous notices, and to reflect nomenclature changes. The proposed rule for the Privacy Act exemptions is also being updated and is published in today's **Federal Register**.

First, in the Central Civil Rights Division Index File and Associated Records system, CRT–001, the Department proposes to allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation. Two other routine use disclosures permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, mediators, negotiators, and other persons performing work or on assignment to the Federal Government. Another routine use will permit the disclosure of information to former employees of the Department for matters in which they were involved. In addition, a revised routine use will permit disclosure of health care-related information obtained during health care-related investigations.

Second, the Department proposes to add five routine use disclosures to Civil Rights Interactive Case Management System, CRT–003. The first routine use allows records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation. Two routine uses are similar to those above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. One routine use will permit disclosure to complainants and victims to provide information about the progress and/or results of an investigation or case. Further, information may be disclosed to the media under certain circumstances unless it would constitute an unwarranted invasion of personal privacy.

Third, the Department proposes to add three routine use disclosures to Registry of Names of Interested Persons Desiring Notifications of Submissions Under Section 5 of the Voting Rights Act, CRT–004. Two routine uses are similar to that above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. Another routine use will allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation.

Fourth, the Department proposes to add three routine use disclosures to Files on Employment Civil Rights Matters from Persons Outside of the Department of Justice, CRT–007. This routine use will permit the disclosure to complainants and victims to provide information about the progress or results of an investigation or case. Two routine uses are identical to that above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. One routine use will permit disclosure to complainants and victims to provide information about the progress or results of an investigation or case.

Fifth, the Department proposes to add two identical routine uses as those above, for disclosure to contractors and former employees, in Civil Rights Division Travel Reports, CRT–009. The other routine use will allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation,

enforcing or prosecuting such violation or law.

In addition, the Civil Rights Division has one system of records, CRT–002, Files of Application for the Position of Attorney with the Civil Rights Division, which is now covered by two government wide systems of records of the Office of Personnel Management (OPM): OPM/GOVT–1, General Personnel Records; and OPM/GOVT–5, Recruiting, Examining and Placement Records (both published on April 27, 2000, at 65 FR 24732–24753). Accordingly, these government wide system notices replace, and the Department hereby removes, on the effective date of this notice, the following notice previously published by an individual Department of Justice component:

Files of Application for the Position of Attorney with the Civil Rights Division, JUSTICE/CRT–002 (previously published on December 17, 1985, at 50 FR 51482).

Finally, the Office of Special Counsel for Immigration Related Unfair Employment Practices was merged into the Civil Rights Division, and its two remaining systems of records are being incorporated into the Civil Rights Division's systems of records. Accordingly, this system notice replaces, and the Department hereby removes, on the effective date of this notice, the following notices previously published by individual Department of Justice components:

Office of Special Counsel, "Central Index File and Associated Records," OSC–001 (previously published on October 17, 1988, at 53 FR 40531); and

Office of Special Counsel, "Special Counsel for Immigration Related Unfair Employment Practices Travel Reports," OSC–003 (previously published on September 15, 1988 at 53 FR 35926).

The Office of Special Counsel's systems of records, OSC–001 and OSC–003, were incorporated into the Civil Rights Division's systems of records, CRT–001 and CRT–009, respectively.

The modified systems of records are printed below.

In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment; and the Office of Management and Budget (OMB), which has oversight responsibility of the Act, requires a 40-day period in which to conclude its review of the system. Therefore, please submit any comments by September 10, 2003. The public, OMB and the Congress are invited to submit comments to: Mary Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, 1331 Pennsylvania Ave., NW., Washington, DC 20530 (1400 National Place Building).

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress.

Dated: July 24, 2003.

**Paul R. Corts,**

*Assistant Attorney General for Administration.*

## JUSTICE/CRT–001

### SYSTEM NAME:

Central Civil Rights Division Index File and Associated Records, CRT–001.

### SYSTEM LOCATION:

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530–0001.

### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

These persons may include: Subjects of investigations, victims, potential witnesses, individuals of Japanese ancestry who were eligible, or potentially eligible, for restitution benefits as a result of their evacuation, relocation, or internment during World War II, and representatives on behalf of individuals and other correspondents on subjects directed or referred to CRT or other persons or organizations referred to CRT in potential or actual cases and matters of concern to CRT, and CRT employees who handle complaints, cases or matters of concern to CRT.

### CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system consist of case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division. The delegated legal duties and responsibilities of each section are described in detail at the Civil Rights Division Web page: *http://www.usdoj.gov/crt/crt-home.html.* In addition to the sections, the Civil Rights Division maintains records related to the duties of the former Office of Redress Administration pertaining to the identification, location and authorization for restitution payments to eligible individuals of Japanese ancestry who were evacuated, relocated or interned during World War II. These restitution payments were authorized by section 105 of the Civil Liberties Act of 1988 (50 U.S.C. App. 1989b). Finally, the names of some individuals, *e.g.*, witnesses, may not yet be on the central indices and may be obtained by direct access to the file jackets. Such file jackets are located within the respective sections of CRT according to the legal subject matter assigned to each CRT section.

### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The records in the system of records are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibility assigned to CRT under the provisions of 28 CFR 0.50, 0.51.

### PURPOSES:

The purposes of this system are to assist all the sections within the Division in maintaining names of Division employees and their case investigation assignments, names of defendants or investigation targets, victims, witnesses or potential witnesses, or other persons or organizations as they relate to potential or actual cases, investigations, and matters of concern to CRT. Other purposes are to assist employees and officials within the Division to review and make decisions in the course of investigations and legal proceedings, to assist the Division in preparing budget requests, to respond to inquiries from outside the Department, and to carry out other authorized Department functions.

### ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(2) In the course of the administration by CRT of a federally mandated program, or the investigation or litigation of a case or matter, a record may be disseminated to a Federal, State or local agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information or has the expertise in an official or technical capacity to assist in the administration of such program or to analyze information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such assistance, information or expert analysis, or to obtain the

cooperation of a prospective witness or informant;

(3) A record relating to a case or matter, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(4) A record relating to a case or matter may be disseminated to an actual or potential party to litigation or the party's attorney (a) for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or (b) in informal discovery proceedings;

(5) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any determination that has been made;

(6) A record relating to a person held in custody or probation during a criminal proceeding or after conviction may be disseminated to any agency or individual having responsibility for the maintenance, supervision or release of such person;

(7) A record may be disseminated to the United States Commission on Civil Rights in response to its request and pursuant to 42 U.S.C. 1975d;

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(9) A record may be disseminated to mediators, negotiators or other persons engaged in efforts to resolve or settle cases or matters pending in the Division as is necessary to enable them to perform their assigned duties;

(10) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(11) Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, health insurers, or associations of health insurers, to promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals, which have jurisdiction over claims against private health plans for allegedly improper disclosures to the Department of Justice of information concerning suspected health care fraud, in determining whether the private health plan qualifies for statutory immunity from civil liability as provided by Section 201 of the Health Insurance Portability and Accountability Act of 1998, codified at 42 U.S.C. 1320a–7c(a)(3)(B)(iii);

(12) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(13) Information may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(14) A record may be disclosed as a routine use to the National Archives and Records Administration (NARA) and to the General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(15) To a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Information in this system is stored on index cards, in file jackets, and on computer disks or tapes.

**RETRIEVABILITY:**

Records are retrieved by the names of individuals or by case numbers assigned to certain cases being investigated by the Department.

**SAFEGUARDS:**

Information in manual and computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

**RETENTION AND DISPOSAL:**

Records are maintained on the system while current and required for official Government use. When no longer needed on an active basis, the paper files are transferred to the Federal Records Center, Suitland, Maryland and some records are transferred to computer tape and stored in accordance with Department security regulations for systems of records. Final disposition is in accordance with records retention schedules approved by NARA.

**SYSTEM MANAGER(S) AND ADDRESS:**

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530–0001.

**NOTIFICATION PROCEDURE:**

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k)(2). Address inquiries to the System Manager listed above.

**RECORD ACCESS PROCEDURES:**

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record retrievable in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), the subject of the case or matter as described under "Categories of records in the system," and any other information which is known and may be of assistance in locating the record, such as the name of the civil rights related case or matter involved, where and when it occurred and the name of the judicial district involved. The requester will also provide a return address for

transmitting the information. Access requests should be directed to the System Manager listed above.

**CONTESTING RECORD PROCEDURES:**

Individuals desiring to contest or amend non-exempt information retrievable in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

**RECORD SOURCE CATEGORIES:**

Sources of information contained in this system may be an agency or person who has or offers information related to the law enforcement responsibilities and/or other statutorily-mandated duties of CRT.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

The Attorney General has exempted parts of this system from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the **Federal Register**. These exemptions apply only to the extent that information in a record pertaining to a particular individual relates to an official federal investigation and/or law enforcement matter. Those files indexed under an individual's name which concern only the administrative management of restitution payments under section 105 of the Civil Liberties Act of 1988 are not being exempted pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

**JUSTICE/CRT–003**

**SYSTEM NAME:**

Civil Rights Interactive Case Management System (ICM).

**SYSTEM LOCATION:**

United States Department of Justice, Civil Rights Division (CRT), 950 Constitution Ave., NW., Washington, DC 20530–0001.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

These persons may include: Complainants, victims, defendants, parties, experts, mediators, Assistant U.S. Attorneys, judges, and individuals or representatives on behalf of individuals in potential or actual cases and matters of concern under jurisdiction of the Civil Rights Division; and CRT employees, including attorneys, paralegals, and professional staff, who handle complaints, cases or matters of concern to CRT.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

(1) Records in this system pertain to a broad variety of cases and matters under the jurisdiction of the CRT relating to disability rights, education, employment, housing, special litigation, voting, criminal, enforcement, and other civil rights laws or matters;

(2) Summary information of these cases or matters is maintained in the system including such information as names of principal parties or subjects, proper case name, case numbers, judicial district, assignments, alleged violation, section of CRT responsible for the matter, and case status, ranging from the preliminary development stage, through investigation, litigation, compliance, appeal, conviction or closure; and

(3) The ICM also has a time reporting system that allows the CRT to capture, analyze and report the professional time attorneys, paralegals and other employees of the Division spend on investigation and case related tasks.

**PURPOSE(S):**

The ICM is designed to track, count and measure all investigations and cases throughout their life cycle. The CRT uses reports generated from this system to provide a profile for each section's activities and to furnish management with a global perspective to the CRT workload. The ICM also has a time reporting system that allows the CRT to capture, analyze and report the level of effort attorneys, paralegals, and professional staff spend on investigation and case related tasks. One purpose of this system is to assist employees and officials of the Department to keep track of resources and professional time devoted to individual assignments to matters and broad categories of cases. Another purpose is to assist the CRT in preparing budget requests and other reports which may be submitted to the Attorney General or to Congress.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

The records in this system are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(3) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or in informal discovery proceedings;

(4) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(5) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(6) A record may be disseminated to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(7) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined

that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(8) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records; and

(9) A record from the system or records may be disclosed to National Archives and Records Administration (NARA) and General Services Administration (GSA) for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records are maintained electronically in the ICM computerized information system.

**RETRIEVABILITY:**

Information is retrieved by name or other identifier assigned to an individual.

**SAFEGUARDS:**

Information contained in the system is unclassified. It is safeguarded and protected in accordance with Departmental security regulations for systems or records. Access to the records is limited to those employees whose official duties require such access in order to perform their duties.

**RETENTION AND DISPOSAL:**

Records are maintained in the system while current and required for official Government use. When no longer needed on an active basis, the records are stored in accordance with Departmental security regulations for systems of records. The disposition schedule is pending approval at NARA.

**SYSTEM MANAGER(S) AND ADDRESS:**

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001.

**NOTIFICATION PROCEDURE:**

Address inquiries to the system manager listed above.

**RECORD ACCESS PROCEDURE:**

A request for access to a record retrievable in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual involved, his or her current address, date and place of birth, and notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), and any other information which is known and may be of assistance in locating the record. The requester should provide a return address for transmitting the information. Access requests should be directed to the System Manager listed above.

**CONTESTING RECORD PROCEDURES:**

Individuals desiring to contest or amend their records should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

**RECORD SOURCE CATEGORIES:**

Information on time-allocation is provided by CRT attorneys, paralegals and professional staff who handle complaints, cases or matters of concern to the CRT. Sources of information contained in this system are those records reflecting all cases or matters under consideration by CRT.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

## JUSTICE/CRT–004

**SYSTEM NAME:**

Registry of Names of Interested Persons Desiring Notification of Submissions under Section 5 of the Voting Rights Act.

**SYSTEM LOCATION:**

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530–0001.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Persons who have requested that the Attorney General send them notice of submissions under Section 5 of the Voting Rights Act of 1965, 42 U.S.C. 1973c.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

The Registry contains the name, address and telephone numbers of interested parties, and, where appropriate, the voting area or areas with respect to which notification was requested by such persons.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

46 FR 877 (1981) codified in 28 CFR part 51, 42 U.S.C. 1973c, 5 U.S.C. 301 and 28 U.S.C. 509, 510.

**PURPOSE(S):**

The purpose is to maintain records in a Registry to identify persons interested in receiving notification of submissions under Section 5 of the Voting Rights Act and to comply with their requests. Section 5, which applies to several states and some counties, requires that any change with respect to voting that a specially covered jurisdiction makes is legally unenforceable unless and until the jurisdiction obtains from the Federal court in the District of Columbia or from the Attorney General a determination that the change is not discriminatory on account of race, color, or membership in a language minority group. If the jurisdiction is unable to prove the absence of discrimination, the Attorney General objects to the change, and it remains legally unenforceable. Further, the Registry may be used to notify the persons listed therein of any proposed changes in the "Procedures for the Administration of Section 5 of the Voting Rights Act of 1965," 46 FR 870 (1981), codified in 28 CFR part 51, and to solicit their comments with respect to any such proposed changes.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings.

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from

the matters of which the complainants or victims complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; and

(9) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Names are stored in a card file system, and an automated addresser.

**RETRIEVABILITY:**

Records in this system are retrievable by the names of interested persons or organizations.

**SAFEGUARDS:**

Information in the system is safeguarded in accordance with Departmental rules and procedures governing access, production and disclosure of any materials contained in its official files.

**RETENTION AND DISPOSAL:**

An individual or organizational name is retained in the Registry until such time as that person or organization requests that the name be deleted.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief, Voting Section, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001.

**NOTIFICATION PROCEDURE:**

Address inquiries to: Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001.

**RECORD ACCESS PROCEDURES:**

This system contains no information about any individual other than as described in Categories of Records above. Persons whose names appear on the Registry may have access thereto or have their names and other information pertaining to them deleted or modified upon a request of the same nature as indicated in 46 FR 877 (1981), codified in 28 CFR part 51.

**CONTESTING RECORD PROCEDURES:**

Same as the above.

**RECORD SOURCE CATEGORIES:**

Sources of information in the Registry are those persons or organizations whose names appear therein by virtue of their having requested inclusion in the Registry pursuant to 46 FR 877 (1981), codified in 28 CFR 51.32.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

## JUSTICE/CRT–007

**SYSTEM NAME:**

Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission.

**SYSTEM LOCATION:**

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue NW., Washington, DC 20530–0001.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Persons seeking employment or employed by a state or a political subdivision of a state who have filed charges alleging discrimination in employment with the Equal Employment Opportunity Commission (hereinafter EEOC) which have resulted in a determination by EEOC that there is probable cause to believe that such discrimination has occurred, and attempts by EEOC at conciliation have failed.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

The system may contain copies of charges filed with EEOC, copies of EEOC's "determination" letters, letters of transmittal from and to EEOC, analyses or evaluations summarizing the charge and other materials in the EEOC file, internal memoranda, attorney notes, and copies of "right to sue" letters issued by CRT. The system may also contain charges related to allegations of employment discrimination by public employers filed by individual complainants which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C. 2000e–5(f) (1) or 5(f) (2), or to allegations of a pattern or practice of violations of the Equal Employment Opportunity Act by a public employer which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C. 2000e–6. If the Department has determined to initiate an investigation or litigate a matter referred by EEOC the records pertaining to that matter are not contained in the system. Such records and their routine uses are described under the notice for the system named: Central CRT Index File and Associated Records/CRT–001.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

The records in this system of records are kept under authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

**PURPOSE(S):**

One purpose of this system is to assist employees and officials of the Department to make decisions regarding the issuance of right to sue letters or make decisions regarding prosecutions of alleged instances of employment discrimination. Another purpose is to assist the Division in preparing budget requests, statistical reports, and other internal functions of the Department.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is

authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; and

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Information in the systems is stored on index cards, in file jackets, and in computer disks which are maintained by the Employment Litigation Section, Civil Rights Division.

**RETRIEVABILITY:**

Information is retrieved primarily by using the appropriate Department of Justice file number, or the name of the charging party, or the state in which the alleged discrimination occurred or through other logical queries to the computer based system.

**SAFEGUARDS:**

Information in manual and computer form is safeguarded and protected in accordance with applicable Departmental security regulations for systems of records. Staff members who are assigned a specific identification code will be able to use the computer or to access the stored information in order to perform their official duties.

**RETENTION AND DISPOSAL:**

If the Department determines not to prosecute a matter referred by the EEOC, the records transmitted with the referral are returned to the EEOC. Other records in the system are kept for routine use by the Department and when no longer needed are sent to the Federal Records Center or are destroyed. Records are retained and disposed of in accordance with item 25 of the General Records Schedule 1 as approved by the Archivist of the United States.

**SYSTEM MANAGER(S) AND ADDRESS:**

Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001.

**NOTIFICATION PROCEDURE:**

Same as the above.

**RECORD ACCESS PROCEDURE:**

A request for access to a record from this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." The request should indicate the state where the alleged employment discrimination took place and the employer to which the charge was related. The requester should also provide the full name of the individual involved, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), any other known information which may be of assistance in locating the record, and a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

**CONTESTING RECORD PROCEDURES:**

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Disclosure of part of the material in this system may be prohibited by 42 U.S.C. 2000e-5(b), 42 U.S.C. 2000e-8(e) and 44 U.S.C. 3510(b). Part of this system is exempted from access and contest under 5 U.S.C. 552a(k) (2).

**RECORD SOURCE CATEGORIES:**

Sources of information in this system are charging parties, information compiled and maintained by EEOC, and employees and officials of the Department of Justice responsible for the disposition of the referral request.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

The Attorney General has exempted the system from 5 U.S.C. 552a (d)(1), (2), (3), and (4) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e), and have been published in the **Federal Register**.

**JUSTICE/CRT–009**

**SYSTEM NAME:**

Civil Rights Division Travel Reports, CRT–009.

**SYSTEM LOCATION:**

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530–0001.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

All persons who have filed travel authorization forms or travel voucher forms for official travel on behalf of CRT.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

The Division's filing system contains information concerning travel expenditures which were recorded on travel authorization forms and travel voucher forms by CRT employees or other persons authorized to travel for CRT and submitted to the Budget and Finance Branch of CRT.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

The records in this system of records are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

**PURPOSE(S):**

One purpose of this system is to assist employees and officials of the Division to measure and track expenditures within the Division. Other purposes are to assist the Division in preparing reports within various sections to control and review expenditures.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(5) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(6) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(7) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; and

(8) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law-criminal, civil or regulatory in nature-the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records are stored in hard copy and electronic form.

**RETRIEVABILITY:**

Records in this system are retrieved by the names of those individuals identified under the caption "Categories of individuals covered by the system."

**SAFEGUARDS:**

Information in the system is unclassified. However, the records are protected in accordance with applicable Department security regulations for systems of records. Records are stored in locked cabinets and access to the computer is limited to those personnel who have a need for access to perform their official duties.

**RETENTION AND DISPOSAL:**

Records are maintained on the system while current and required for official Government use. When no longer needed on an active basis, the records are transferred to computer tape and stored in accordance with Departmental security regulations for systems of records. Final disposition will be in accordance with records retirement or destruction as scheduled by NARA in General Records Schedule 9.

**SYSTEM MANAGER(S) AND ADDRESS:**

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001.

**NOTIFICATION PROCEDURE:**

Same as the above.

**RECORD ACCESS PROCEDURES:**

Requests by former employees for access to records in this system may be made in writing with the envelope and letter clearly marked "Privacy Act Request." The request should clearly state the dates on which official travel was taken. The requestor should also provide the full name of the individual involved, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), any other known information which may be of assistance in locating the record, and a return address for transmitting the information. Access requests will be directed to the System Manager. Present employees may request access by contacting the System Manager directly.

**CONTESTING RECORD PROCEDURES:**

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought.

**RECORD SOURCE CATEGORIES:**

Sources of information are CRT employees and other authorized persons who file travel authorization and travel voucher forms.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

[FR Doc. 03–20342 Filed 8–8–03; 8:45 am]
BILLING CODE 4410–13–P

## DEPARTMENT OF LABOR

### Mine Safety and Health Administration

### Proposed Information Collection Request Submitted for Public Comment and Recommendations; Explosive Materials and Blasting Units

**ACTION:** Notice.

**SUMMARY:** The Department of Labor, as part of its continuing effort to reduce

# Department of Justice
# Justice Management Division


## Privacy Impact Assessment
for the
Justice Enterprise File Sharing System

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

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

Date approved: [November 30, 2017]

(May 2015 DOJ PIA Form)

# EXECUTIVE SUMMARY

The Justice Enterprise Files Sharing (JEFS) system uses the Box Incorporated ("Box")[1] Software as a Service (SaaS) capability[2] as a transport infrastructure for users to share securely most types of files within Department of Justice (DOJ or the Department) Components, between DOJ Components, and with external entities who have authority to access information maintained by the Department. The JEFS system can function across multiple platforms including smartphones, tablets, and workstations, anywhere inside or outside the DOJ network. The Department utilizes JEFS as a transport infrastructure only, and the Department has not designated the JEFS system as an official record-keeping system, a document archival system, or a document backup system.

The Department conducted this Privacy Impact Assessment (PIA) because the personally identifiable information (PII) collected, used, and maintained includes names, email addresses, and audit log information of DOJ employees and contractors, as well as names, email addresses, mobile phone numbers, and audit log information of non-DOJ end-users. Additionally, documents transferred through JEFS may include significant quantities of personal information relating to the substantive work of the Department. Because of the varied nature of the Department's work, documents transferred through JEFS could conceivably include almost any type of unclassified PII information. This PIA covers all Department Components' instances of JEFS.

## Section 1: Description of the Information System

(a) The purpose that the records and/or system are designed to serve;

DOJ implemented JEFS to simplify secure internal and external file sharing with key stakeholders and third party organizations, (e.g., expert witnesses, co-counsel, and local law enforcement officers), and to support mobile and offline access to files regardless of location or device. The Department utilizes JEFS as a transport infrastructure only, and the Department has not designated JEFS as an official record-keeping system, a document archival system, or a document backup system.

(b) The way the system operates to achieve the purpose(s);

JEFS is a specially configured implementation of Box's SaaS capability that underwent a

---

[1] Box Inc. provides an enterprise content management platform that allows users to share and access files, while establishing specific data governance and retention policies for specific clients, such as DOJ. More information on Box can be found at: https://www.box.com/home.

[2] "SaaS" capabilities provide consumers with a provider's applications running on a cloud infrastructure. National Institute for Standards and Technology (NIST), Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. "The applications are accessible from various client devices through either a thin client interface, such as a web browser . . . or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings." *Id.*

rigorous security assessment and meets DOJ security requirements. JEFS enables users to upload up to 15 gigabytes of most file types—documents, videos, photos, etc.—from a phone, tablet or computer. Users can then access those files for up to 60 days[3] from anywhere through the DOJ network or over the Internet.

Box manages the hardware and software cloud environment, [4] and DOJ manages the front-end application of each instance of JEFS.

Each individual DOJ Component (e.g., the Federal Bureau of Investigation, the Bureau for Alcohol, Tobacco, Firearms, and Explosives, the Drug Enforcement Administration) manages its own JEFS instance, and purchases its own licenses directly from the vendor using a DOJ Blanket Purchase Agreement (BPA). Each Component also manages its own service desk and account administration. Accounts for users from DOJ Components that do not have their own JEFS instance are created under the Justice Management Division (JMD) JEFS instance. This PIA covers all the Department's JEFS instances.

(c) The type of information collected, maintained, used, or disseminated by the system;

The JEFS system collects, maintains, and uses the following information for DOJ users: user name and DOJ email address. The JEFS system collects, maintains, and uses the following information for non-DOJ users: user name, email address, and mobile phone number.

As detailed below in Section 6, the JEFS system also maintains audit logs of JEFS user activity such as logins, uploads, downloads, file rename, Internet Protocol (IP) address, and browser.

The particular data that passes through JEFS is Sensitive-But-Unclassified (SBU) at its highest classification. JEFS is not authorized to process, store, or transmit classified data. JEFS has a Security Categorization of Moderate based on the Federal Information Processing Standard Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.[5]

Because of the varied nature of the Department's work, the files shared via the JEFS system could conceivably include any type of SBU Moderate information; it is therefore not possible to list with certainty every item of information that users could potentially share via the system.

---

[3] Under limited, case-by-case circumstances, the JEFS System Owner, in consultation with the DOJ Office of the Chief Information Officer, Cybersecurity Services Staff, may grant a waiver to extend the 60-day retention period.

[4] "Cloud computing" is defined by NIST as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." *Id.* A "cloud environment" or "cloud infrastructure" is the "collection of hardware and software that enables the five essential characteristics of cloud computing." *Id.*

[5] A Security Categorization of Moderate means "the loss of confidentiality, integrity, or availability to this system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." *See* NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

However, JEFS will only handle information that the DOJ has the authority to share. The Department may share information within DOJ Components, between DOJ Components, and with external entities who have authority to access information maintained by the Department to accomplish an authorized function.

The JEFS system collects metadata about shared files, such as the file create date, but not the content of the files shared. Authorized files accessed for transport in and out of the JEFS system are deleted after 60 days through automated means.[6]

(d) Who has access to information in the system;

Access to JEFS is restricted to DOJ employees and contractors, and approved users from external entities outside DOJ. A user is granted a JEFS account only when approved by the DOJ Component Authorizing Official or designee. Additionally, some DOJ Components impose further requirements that must be met prior to granting a JEFS account. Only the DOJ JEFS Administrators have access to the information collected by the system as described in section 1.c.

(e) How information in the system is retrieved by the user;

Information in the JEFS system can be accessed using multiple platforms including smartphones, tablets, and desktop computers. Once authenticated into the JEFS system, JEFS users have access to files to which they have been granted explicit authorization (e.g., read only, edit, lock, password protect.) DOJ JEFS Administrators can retrieve audit log information by a JEFS user's name or email address. Once a user is successfully authenticated and logs into JEFS, the user sees the JEFS interface. A user can then use one of two methods to upload files and folders into JEFS: either a "drag and drop" method, or through a search for files through the user's file browser. To access a file already in JEFS, the user clicks on the desired folder or file.

(f) How information is transmitted to and from the system;

Every file is encrypted in transit between the user (independent of platform) and Box data centers with high-grade Secure Sockets Layer (SSL) encryption, compliant with the FIPS Publication 140-2.[7] Once encrypted data reaches the Box network, files are encrypted when stored ("at rest") at all times using the 256-bit Advanced Encryption Standard (AES).[8] All physical co-location facilities used as the primary processing facilities are located within the United States.

---

[6] *See supra* note 3.
[7] NIST FIPS 140-2 can be found at: http://csrc.nist.gov/groups/STM/cmvp/standards.html.
[8] AES "specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data." NIST FIPS 197, *Advanced Encryption Standard (AES)* (Nov. 2001), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Specifically, the AES algorithm "is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext." *Id.*

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

The JEFS system interfaces with the DOJ's Active Directory Federation Services for the authentication of DOJ JEFS users when accessing the JEFS system from within the DOJ network.

(h) Whether it is a general support system, major application, or other type of system;

The JEFS system is categorized as a Major Application.

# Section 2: Information in the System

## 2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Specific to JEFS user accounts, the JEFS system collects and maintains the following information:

- For DOJ JEFS users: User name, DOJ email address, IP address and browser
- For non-DOJ JEFS users: User name, email address, mobile phone number, IP address and browser. The mobile phone number is required because non-DOJ must go through a second factor authorization through Short Message Service texts when logging in from an unknown device.
- JEFS also maintains audit logs of user activity such as logins, uploads, and downloads.

Additionally, documents transferred through JEFS may include significant quantities of personal information relating to substantive work of the Department. Because of the varied nature of the Department's work, the JEFS system could be used to share any SBU Moderate information that a DOJ user has authorization to disclose to a recipient user. Consequently, it is not possible to list with certainty every item of information that will be disseminated by the system. Therefore, the items of the information checked below are limited to end-user account information and audit log information maintained by the JEFS system. Specific to the files shared via JEFS, the JEFS system collects metadata about files, such as the file create date, but not on the content of the files.

| **Identifying numbers** | | | | | |
|---|---|---|---|---|---|
| Social Security | | Alien Registration | | Financial account | |
| Taxpayer ID | | Driver's license | | Financial transaction | |
| Employee ID | | Passport | | Patient ID | |
| File/case ID | | Credit card | | | |

| Identifying numbers | |
|---|---|
| Other identifying numbers (specify): | |

| General personal data | | | | | |
|---|---|---|---|---|---|
| Name | X | Date of birth | | Religion | |
| Maiden name | | Place of birth | | Financial info | |
| Alias | | Home address | | Medical information | |
| Gender | | Telephone number | X | Military service | |
| Age | | Email address | | Physical characteristics | |
| Race/ethnicity | | Education | | Mother's maiden name | |
| Other general personal data (specify): | | | | | |

| Work-related data | | | | | |
|---|---|---|---|---|---|
| Occupation | | Telephone number | X | Salary | |
| Job title | | Email address | X | Work history | |
| Work address | | Business associates | | | |
| Other work-related data (specify): | | | | | |

| Distinguishing features/Biometrics | | | | | |
|---|---|---|---|---|---|
| Fingerprints | | Photos | | DNA profiles | |
| Palm prints | | Scars, marks, tattoos | | Retina/iris scans | |
| Voice recording/signatures | | Vascular scan | | Dental profile | |
| Other distinguishing features/biometrics (specify): | | | | | |

| System admin/audit data | | | | | |
|---|---|---|---|---|---|
| User ID | | Date/time of access | X | ID files accessed | |
| IP address | X | Queries run | | Contents of files | |
| Other system/audit data (specify): | Browser type and modifications to JEFS system settings. | | | | |

| Other information (specify) |
|---|
| |

## 2.2 Indicate sources of the information in the system. (Check all that apply.)

The sources of the information in the JEFS system come from two distinct JEFS users: DOJ users and non-DOJ users. DOJ users include both DOJ employees and DOJ contractors. DOJ users are required to provide their name and a DOJ email address to obtain a JEFS account.

Non-DOJ users include employees of other federal agencies, employees of state or local government agencies, employees of a private company or law firm, or other external entities that have authorization to access particular information shared by DOJ users or authorization to transfer information to DOJ users. Non-DOJ users provide name, email address and mobile phone to obtain a JEFS account.

JEFS users upload files into JEFS as part of their substantive work for the Department. Though such files may come from any source(s), the JEFS system retains beyond the 60-day retention period only metadata about shared files,[9] such as the file create date, but not the content of the files shared. In JEFS, every file is encrypted in transit (a process that starts when the user clicks on the file to be uploaded, until it reaches the cloud service provider data centers) with high-grade SSL encryption, compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

| **Directly from individual about whom the information pertains** | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | | Online | X |
| Telephone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ components | X | Other federal entities | X |
| State, local, tribal | X | Foreign | X | | |
| Other (specify): | | | | | |

| **Non-government sources** | | | | | |
|---|---|---|---|---|---|
| Members of the public | X | Public media, internet | X | Private sector | X |
| Commercial data brokers | X | | | | |
| Other (specify): | | | | | |

## 2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy.

A potential threat to privacy in light of the information collected is that the system will collect

[9] *See supra* note 3.

and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. JEFS is a transport infrastructure that does not exercise control over the contents of information shared; however, there are existing technical, administrative, and physical limits on the type of information that may be collected, including but not limited to, the statutory protections afforded certain information under the Privacy Act of 1974, as amended ("Privacy Act"), and DOJ policies.

JEFS is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, authorized files accessed for transport in and out of the JEFS system are deleted in 60 days through automated means.[10] On a case-by-case basis, depending on the DOJ Component operating procedures, the deleted files may be restored by the DOJ Component JEFS Administrator up to 7 days after the automated deletion.

To prevent unauthorized access to JEFS, DOJ staff (employees and contractors) and approved users from external entities outside DOJ can have access to the JEFS system if approved by the DOJ Component Authorizing Official or designee, as detailed in Section 6. Additionally, some DOJ Components impose further requirements that must be met prior to granting a JEFS account.

To further mitigate potential risks associated with collecting or maintaining more information than is necessary to accomplish the Department's official duties, all JEFS inactive accounts are deleted after 90 days of inactivity.

Additionally, because JEFS users use the system to help carry out the Department's various missions, the type of files transported through the system are governed by the various authorities delineating component missions and authorizing the collection and maintenance of information to carry out such missions. These authorities are listed in the various Privacy Act system of records notices (SORN) that apply to the records maintained in a system of records transported via JEFS, depending on the nature of such files and how the information on the files is retrieved.

For information about the security controls that the Department applied to JEFS that assist in mitigating threats related to the collection of PII, please see the responses to questions 6.1 and 6.2, below.

# Section 3: Purpose and Use of the System

## 3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

The JEFS system is only used as a transport infrastructure. It offers high volume short-term capabilities to share documents and most types of files among individuals within DOJ

[10] *See supra* note 3.

Components, between DOJ Components, and with external entities who have authority to access particular information shared by the Department. DOJ personnel use the JEFS system file sharing functionality in furtherance of the various missions of DOJ components. The JEFS system is not designated as an official record-keeping system, a document archival system, or a document backup system.

| Purpose | | | |
|---|---|---|---|
| X | For criminal law enforcement activities | X | For civil enforcement activities |
| | For intelligence activities | X | For administrative matters |
| X | To conduct analysis concerning subjects of investigative or other interest | X | To promote information sharing initiatives |
| X | To conduct analysis to identify previously unknown areas of note, concern, or pattern. | X | For administering human resources programs |
| X | For litigation | | |
| X | Other (specify): To assist in the secure sharing of SBU Moderate files by DOJ Components to entities that have appropriate authorization to access such information in support of DOJ Component activity. | | |

## 3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The breadth of the DOJ mission and the DOJ Components, including civil and criminal law enforcement, requires secure, timely, and effective communications and information sharing in support of the areas checked in question 3.1. DOJ personnel use the JEFS system file sharing functionality in furtherance of the various missions of DOJ components. Examples may include:

- to send and receive information from external entities including other US government agencies and other law enforcement organizations;
- to perform instant DOJ staff-to-staff transfer of law enforcement data that is typically too large to email;
- to share information with external entities including expert witnesses, opposing counsel, etc.;
- to exchange information with courts;
- to share information with external entities including vendors, consultants, attorneys, etc.;
- to transfer information to mobile devices or DOJ laptops for access to information in locations such as courts, senior leadership briefings, etc.;
- to receive job applicant materials;
- to deliver information to DOJ staff in other components;
- to exchange IT-related files such as source code, log files, etc.; and
- to disseminate training materials.

## 3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

| | Authority | Citation/Reference |
|---|---|---|
| X | Statute | 5 U.S.C. § 301; 44 U.S.C. § 3101 |
| | Executive Order | |
| | Federal Regulation | |
| X | Memorandum of Understanding/agreement | Justice Enterprise File Sharing Memorandum of Agreement between DOJ and Components. |
| X | Other (summarize and provide copy of relevant portion) | Various DOJ component mission authorities (including statutes, Executive Orders, and regulations).<br><br>DOJ Order 0904 – Cybersecurity Program;<br>DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems;<br>DOJ Order 0903 Information Technology Management;<br>DOJ Order 2880.1C – Information Resources Management Program 1 C Chapter 2, section 16. |

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

The JEFS system is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, authorized files accessed for transport in and out of the JEFS system are deleted in 60 days through automated means.[11]

Box Inc. stores audit logs of system administration/audit information (including user account information) for a period of 7 years or until the front-end application/system is removed. In accordance with the DOJ IT Security Standards, JEFS audit logs of administration/audit information (including user account information) sent to DOJ are retained for a minimum of 1 year online and 30 days offline (in backup storage). The Department would ingest logs into the

[11] *See supra* note 3.

DOJ Justice Management Division, Cybersecurity Services Staff Splunk instance.[12]

## 3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The JEFS system provides users with the ability to share files over the web, via a standard web-browser, and through a mobile interface such as a native mobile application (available on iOS, Android, Windows mobile OS, and Blackberry devices). Potential threats to privacy when sharing files via the JEFS system include unauthorized disclosure of information.

To ensure authorized use of JEFS, DOJ staff and approved users from external entities outside DOJ can have access to the JEFS system if approved by the DOJ Component Authorizing Official or designee. Additionally, some Components may impose further requirements prior to granting a JEFS account.

To ensure that the information is handled, retained, and disposed of appropriately, users take mandatory computer training annually which includes training on the Privacy Act and the Cybersecurity Executive Branch Order. Additionally, JEFS users agree at least annually to the JEFS Terms of Usage that include General Rules of Behavior and a link to the Department of Justice Website Privacy Policy.[13]

To protect files shared via JEFS, the system has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a particular file. Every time a user attempts to access a file or folder (by clicking on the file on the JEFS interface which is displayed after the user has successfully authenticated into the system), JEFS uses these permissions to verify that a user has explicit authorization to interact with the file and what specific interaction permissions (e.g., read-only). This process ensures that a user has access only to the files or folders to which the user is allowed and that the user is restricted to the authorized type of interaction with the specific files or folders.

In JEFS, every file is encrypted in transit (the process that starts when the user clicks on the file to be uploaded, until it reaches the cloud service provider data centers) with high-grade SSL encryption, compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. All physical co-location facilities used as the primary

---

[12] The Department's Splunk instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

[13] The DOJ Website Privacy Policy can be found here: https://www.justice.gov/doj/privacy-policy.

processing facilities are located within the United States. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

JEFS audit logs are available on a read-only mode to designated DOJ JEFS privileged users. DOJ JEFS privileged users such as JEFS Administrators and JEFS Information System Security Officers review JEFS audit logs for security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity. JEFS audit logs are automatically monitored by Box's Security Incident and Event Management (SIEM) tool. Any alteration of JEFS audit logs would be flagged by the SIEM.

Authorized files accessed for transport in and out of the JEFS system are deleted after 60 days through automated means.[14] In addition, each DOJ Component with a JEFS instance can further customize the security and permissions of its files. For example, DOJ Components with a JEFS instance can specify when a user can only upload files into a folder without the ability to view other files on the folder; specify that a file can only be shared only with users with a usdoj.gov domain email address; or prohibit downloads of a certain file. Overall, JEFS users are given only the privileges they need to access a file and the file is deleted through automated means.

Additionally, the JEFS system has automated functionality to place files that may contain Social Security Numbers (SSNs) or files with words/phrasing similar to security markings higher than SBU (e.g., Top Secret) into a restricted "Quarantine" area. The files will then require action from a JEFS Administrator before they become available for use.

For a list and description of security controls that have been put into place to safeguard against these and other risks (including mandatory training for system users regarding appropriate handling of information and automatic purging of information), please see the responses to questions 6.1 and 6.2.

# Section 4: Information Sharing

## 4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | Case-by-case | Bulk transfer | Direct access | Other (specify) |
| Within the component | X | | | |
| DOJ components | X | | | |
| Federal entities | X | | | |

[14] *See supra* note 3.

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | Case-by-case | Bulk transfer | Direct access | Other (specify) |
| State, local, tribal gov't entities | X | | | |
| Public | X | | | |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | X | | | Foreign nationals may obtain a JEFS account with approval from both the Department of Justice Chief Information Officer (CIO) and the Department of Justice Security Officer (DSO). |
| Other (specify): | X | | | Any other external entity that is authorized to establish a JEFS account and has the authority to receive information maintained by DOJ, such as outside experts or parties in litigation. |

**4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)**

To prevent or mitigate threats to privacy in connection with the disclosure of information, each DOJ Component that operates a JEFS instance signs a JEFS Memorandum of Agreement (MOA) with JMD. In the JEFS MOA, the DOJ Component agrees to comply with the requirements of the JEFS Authority to Operate (ATO). The DOJ Component further certifies that its own policies, if any, governing end users' access to, or appropriate use, handling, dissemination, and/or destruction of information pertaining to JEFS align with DOJ system requirements.

In addition, each user must also agree at least annually to the DOJ Terms of Usage that include the DOJ General Rules of Behavior and a link to the Department of Justice Website Privacy Policy. Additionally, every page in JEFS, including the JEFS login page, displays a link to the Department of Justice Website Privacy Policy.

By Department Order, all DOJ users working on Department systems including JEFS, must receive an annual Computer Security Awareness Training (CSAT) course. The CSAT course includes information on certain federal information privacy laws and requirements, such as the Privacy Act and requirements for proper handling of PII.

JEFS has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction (e.g. read-only) with the specific files or folders.

To prevent or mitigate threats to privacy in connection with the disclosure of information, the JEFS system has automated functionality to place files that may contain SSNs or files with words/phrasing similar to security markings higher than SBU (e.g. Top Secret) into a restricted "Quarantine" area. These files will then require action from a JEFS Administrator before they become available for use. Additionally, responses to potential unauthorized disclosures or data breaches are covered in vendor contracts.

JMD maintains the security certification and accreditation of the system. For a list and description of security controls that have been put in place in order to prevent or mitigate threats to privacy in connection with the disclosure of information, as well as to safeguard against other threats to privacy, please see the responses to questions 6.1 and 6.2.

## Section 5: Notice, Consent, and Redress

### 5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

| | | |
|---|---|---|
| X | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. | |
| X | Yes, notice is provided by other means. | Specify how: A warning banner notifies JEFS end-users at login that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in such information.<br><br>Additionally, once a year, JEFS users must consent to the JEFS Terms of Use and the DOJ Rules of Behavior. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system, |

| | | |
|---|---|---|
| | | a document archival system, or a document backup system. As such, the notification to individuals is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions. |
| | No, notice is not provided. | Specify why not: |

## 5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

| | | |
|---|---|---|
| X | Yes, individuals have the opportunity to decline to provide information. | Specify how: Specific to information collected by JEFS, such as the user name and email address, DOJ personnel may choose to use a means to share files other than the JEFS system (e.g. email, phone, fax, other systems, etc.). Moreover, non-DOJ individuals may choose not to use the JEFS system to share files with DOJ users. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system, a document archival system, or a document backup system. As such, the opportunity to decline to provide information contained in the files shared via JEFS is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions. |
| | No, individuals do not have the opportunity to decline to provide information. | Specify why not: |

## 5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of the information. | Specify how: JEFS users provide consent when they agree to the JEFS Terms of Usage and the DOJ Rules of Behavior. Specific to files shared via JEFS, the JEFS system is only used as a transport infrastructure with no processing and it is not designated as an official record-keeping system, a document archival system, or a document backup |

| | | |
|---|---|---|
| | | system. As such, the opportunity to decline to consent to particular uses of the information contained in the files shared via JEFS is governed by the various authorities delineating DOJ Component missions and authorizing the collection and maintenance of information to carry out such missions. |
| | No, individuals do not have the opportunity to consent to particular uses of the information. | Specify why not: |

## 5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

To provide transparency and allow JEFS users to understand how their communications and other information are handled, the following is in place:

- The DOJ security-warning banner is displayed on the login screen that JEFS users see when they log into the JEFS system. The DOJ warning banner informs users that any information that they transmit through a computer or mobile device, including information transmitted through JEFS, may be monitored, intercepted, searched, and/or seized by the Department, and that JEFS users therefore have no reasonable expectation of privacy while using the system.

- Additionally, the JEFS Terms of Usage is also displayed when a user first logs in and at a minimum annually thereafter. The JEFS Terms of Usage inform users that any information that they transmit through a computer or mobile device, including information transmitted through JEFS, may be monitored, intercepted, searched, and/or seized by the Department, and that JEFS users therefore have no reasonable expectation of privacy in such communications.

- The JEFS Account Request Form template includes the DOJ Rules of Behavior (ROB) that users sign prior to submitting the account request. The DOJ ROB explains that acknowledgment of the DOJ ROB also indicates consent to monitoring, recording, and collection of data on all DOJ devices for law enforcement purposes.

JEFS system is only used as a transport infrastructure and is not designated as an official record-keeping system. Notice and opportunity to consent on individual information that may be contained on the files shared is governed by the various authorities delineating Component

missions and authorizing the collection and maintenance of information to carry out such missions.

Moreover, as noted above, JEFS is a transport infrastructure and because of the varied nature of the Department's work, the files shared via the JEFS system could conceivably include any type of SBU Moderate information. However, to the extent that content contained in such communications are protected by federal law, including the Privacy Act, notice is provided by various DOJ Privacy Act systems of records notices (SORNs), which apply depending on how information is retrieved. These notices and documents are published in the Federal Register and available to the general public, as described in Section 7, below.

Finally, a link to the Department of Justice Website Privacy Policy is displayed in the footer of every page in the JEFS system.

# Section 6: Information Security

## 6.1 Indicate all that apply.

| | |
|---|---|
| X | The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: May 27, 2015<br><br>If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: |
| X | A security risk assessment has been conducted. |
| X | Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The Box SaaS has a FedRAMP authorization[15] at the Moderate Impact level. Box utilized a FedRAMP Third-Party Assessment Organization (3PAO) to perform an independent security assessment against a FISMA moderate security baseline. JEFS has a security categorization of Moderate. The identified DOJ security controls have been tested and implemented to protect against risks identified in the security risk assessment which includes those listed in DOJ Security Assessment and Authorization Handbook v. 8.4, providing the framework and direction for performing security assessments and authorizations of all DOJ IT systems, as well as those listed in response to question 6.2. The Justice Management Division, Service Delivery Staff, Application and Web Services Staff is responsible for maintaining the enterprise security Authorization To Operate (ATO) of JEFS. To leverage the JEFS enterprise ATO, Components sign the JEFS Memorandum of Agreement and adhere to the ATO and associated Standard Operating Procedures. |

[15] The Federal government's FedRAMP program provides a "cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies." More information on the FedRAMP program can be found at: https://www.fedramp.gov.

| | |
|---|---|
| X | Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: DOJ IT security standards, which include monitoring, testing, and evaluation requirements, have been applied to the system. The security controls for JEFS are assessed and/or reviewed annually at a minimum, using the Cyber Security Assessment and Management application, to include all three classes: management, operational, and technical. The assessment and review/update is documented in said system. See the response to question 6.2 for additional information on monitoring, testing, and evaluation. |
| X | Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: JEFS provides reporting and audit trail of account activities on both user accounts and files. Audit logs can only be accessed by authorized staff as required to ensure compliance with security requirements. The JEFS system does not collect data on the content of the files shared. The JEFS system has application access controls that limit access to files and folder using role-based permissions to safeguard against unauthorized access, use, and disclosure of information. |
| X | Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. |
| X | Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy. |
| | The following training is required for authorized users to access or receive information in the system: |
| X | General information security training |
| | Training specific to the system for authorized users within the Department. |
| | Training specific to the system for authorized users outside of the component. |
| X | Other (specify): As further defined by each DOJ Component. |

## 6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The following access and security controls have been utilized to protect privacy and reduce the risk of unauthorized access and disclosure:

- JEFS has a security categorization of FISMA Moderate. The Box SaaS has a FedRAMP authorization at the Moderate Impact level. DOJ has assessed and implemented all applicable security controls that are the DOJ responsibility for a FISMA Moderate baseline.

- The JEFS system is accessible to DOJ employees, contractors, and approved users from external entities outside DOJ, only when approved by the DOJ Component Authorizing Official or designee. Additionally, some Components impose further requirements that must be met prior to granting a JEFS account.

- JEFS has specific controls in place that ensure users can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions

associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction with the specific files or folders.

- In JEFS, every file is encrypted in transit with high-grade SSL encryption compliant with FIPS 140-2. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. All physical co-location facilities used as the primary processing facilities are located within the United States. The cloud service provider personnel can see the encrypted files and metadata about those files, such as the file create date, but not the information within the files themselves.

- To protect privacy and reduce the risk of unauthorized access and disclosure, the JEFS system has automated functionality to place files that may contain SSNs or files with words/phrasing similar to security markings higher than SBU (e.g. Top Secret) into a restricted "Quarantine" area. The files will then require action from a JEFS Administrator before they become available for use.

- All users must complete CSAT annually, as well as read and agree to comply with DOJ Information Technology Rules of Behavior and the JEFS Terms of Usage, prior to accessing the JEFS system and annually thereafter. Additionally, JEFS administrators must complete JEFS Administrator training, which includes JEFS security training.

- JEFS is configured with automatic audit logging which includes logging of JEFS Administrator activity. Further, logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. JEFS audit logs can only be accessed on read-only mode by authorized DOJ JEFS users with privileged access. JEFS audit logs are automatically monitored by the Box SIEM tool, which would flag any alteration of JEFS audit logs.

- Responses to potential unauthorized disclosures or data breaches are covered in vendor contracts and system rules of behavior in order to ensure appropriate procedures and reporting.

# Section 7: Privacy Act

## 7.1 Indicate whether a system of records is being created or has been created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

| | |
|---|---|
| X | Yes, and this system is covered by an existing system of records notice.<br><br>Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:<br><br>• JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009), and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017);<br>• JUSTICE/DOJ-002, Department of Justice Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017);<br>• Other published DOJ system of records notices depending on the nature of information in the communication or collaboration document and how the information is retrieved. These SORNs apply only to the extent of the information for JEFS accounts as described in section 2.1. |
| | Yes, and a system of records notice is in development. |
| | No, a system of records is not being created. |

## 7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

JEFS Administrators can retrieve JEFS user account information and audit log information by user account name or user account email address.

JEFS has built controls that ensure every user can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, JEFS uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed; and that the user is restricted to the authorized type of interaction (e.g. read-only) with the specific files or folders.

**From**: Okwesa, Carolyn (CRT) (b)(6)
**Sent**: 8/27/2025 1:05:33 PM
**To**: Kagle, Kilian (CRT) [(b)(6)]
**CC**: Bryce, Amanda (CRT) [A(b)(6)]
**Subject**: Privacy Related/data sharing

Good morning Kilian,
Voting has reached out to OITC for guidance regarding Privacy Act/data sharing where data contains PII from states. Some states have questions, and Voting would like to respond to those questions today. I'm hoping you will have time to meet with Amanda and I at 11am. I'll send an invite shortly.
Thank you,
Carolyn

Carolyn Okwesa
Project Manager (Contractor) | Office of Information Technology and Cybersecurity
U.S. Department of Justice | Civil Rights Division | Administrative Management Section
(b)(6)
(b)(6)

**From:** Bruzzone, Callie (CRT) [(b)(6)]
[(b)(6)]
**Sent:** 9/4/2025 11:13:32 PM
**To:** Mellett, Timothy F (CRT) [(b)(6)]; Wake, Brittany (CRT) [(b)(6)]
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields
**Attachments:** 2025.9.04 UT Privacy Letter.docx

Suggested draft attached.

---

**From:** Mellett, Timothy F (CRT) <[(b)(6)]>
**Sent:** Thursday, September 4, 2025 4:21 PM
**To:** Bruzzone, Callie (CRT) <[(b)(6)]>; Wake, Brittany (CRT) [(b)(6)]
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

You can share: Yes, 52 U.S.C. § 21083(a)(2) Computerized list maintenance under both A and B; 52 U.S.C. § 21083(a)(5)(A) Requiring DL/SSN4

**(b)(5)**

You can share No, Privacy Act prohibits sharing with outside agencies. As would the data sharing agreement.

You can share CRA provides authority for last 22 months, but we have authority under NVRA and HAVA for these requests. 8(i) for NVRA and our enforcement authority. For HAVA, we cite the enforcement authority.

---

**From:** Bruzzone, Callie (CRT) [(b)(6)]
**Sent:** Thursday, September 4, 2025 4:15 PM
**To:** Mellett, Timothy F (CRT) <[(b)(6)]>; Wake, Brittany (CRT) [(b)(6)]
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Thank you – what of this information can I include in the letter?

---

**From:** Mellett, Timothy F (CRT) <[(b)(6)]>
**Sent:** Thursday, September 4, 2025 3:49 PM
**To:** Bruzzone, Callie (CRT) <[(b)(6)] Wake, Brittany (CRT) <[(b)(6)]>
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

See the answers in blue below.

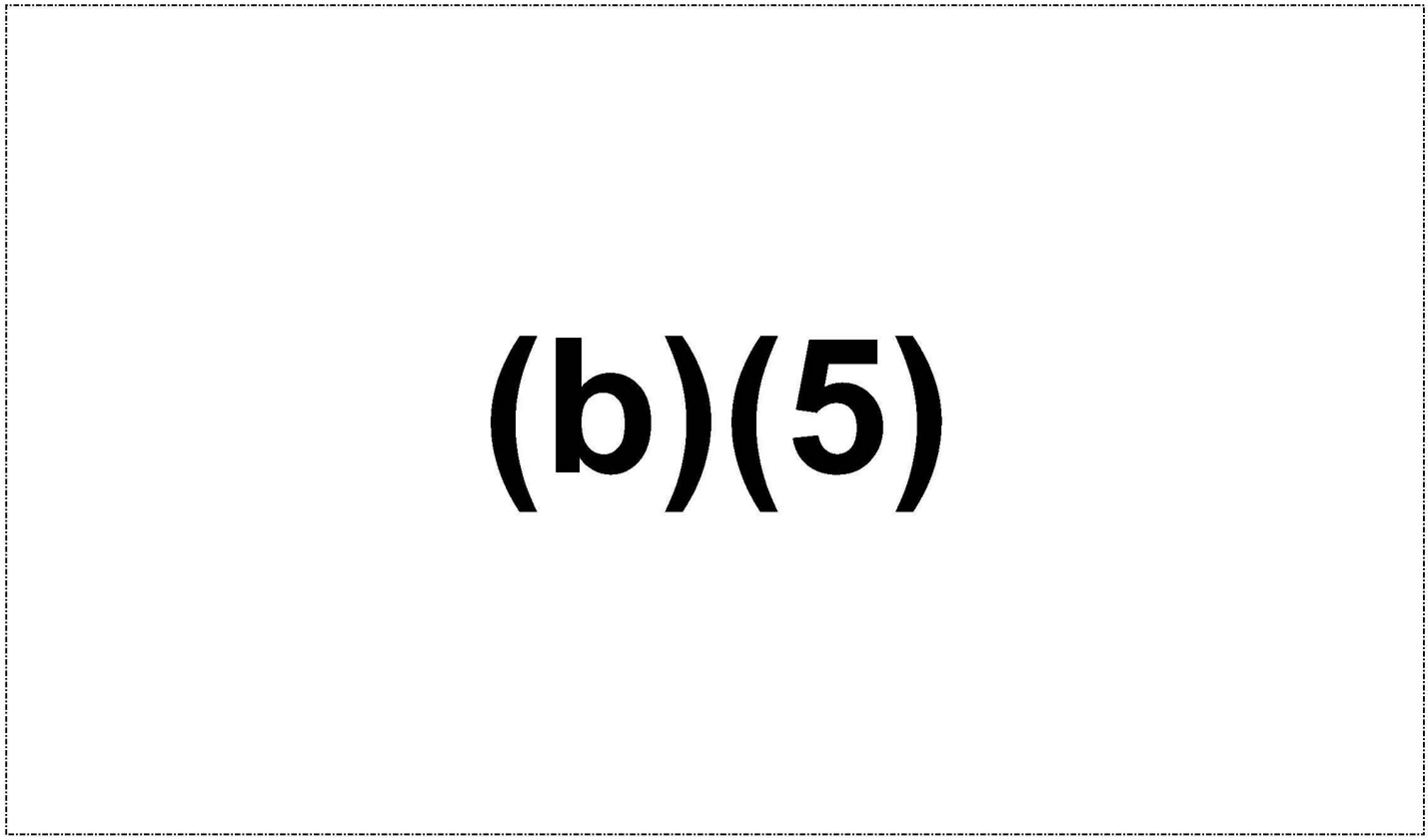
---

**From:** Bruzzone, Callie (CRT) <[(b)(6)]
**Sent:** Thursday, September 4, 2025 2:14 PM
**To:** Mellett, Timothy F (CRT) <[(b)(6)]>; Wake, Brittany (CRT) [(b)(6)]
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Tim,

I wanted to check in on this task, because it has become a bit more complicated than I expected. UT asks specific questions that are unaddressed in the TN model letter. I am not sure of the Section's position on some of these concerns. Here are the specific questions and what I know about each. Please let me know if my understanding is accurate and what to communicate to UT.

(b)(5)




Thank you for your help with these questions.

Best,

Callie

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Wednesday, September 3, 2025 9:49 AM
**To:** Bruzzone, Callie (CRT) <(b)(6)>; Wake, Brittany (CRT) <(b)(6)>
**Subject:** FW: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Callie and Brittany,

See the attached correspondence from Utah. Please prepare a privacy letter for Utah using the letter to Tennessee as a model. Please send me a draft later today. Thanks,

Tim

---

**From:** Ryan Cowley <(b)(6)
**Sent:** Friday, August 29, 2025 6:54 PM
**To:** Gates, Michael (CRT) <(b)(6)>
**Cc:** (b)(6)@utah.gov; Riordan, Maureen (CRT) <(b)(6)>; Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** Re: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Mr. Gates, please find attached my response to your email dated August 22. 2025.

**Ryan Cowley** | **Director of Elections**
OFFICE OF LIEUTENANT GOVERNOR
DEIDRE M. HENDERSON
LTGOVERNOR.UTAH.GOV
801-538-1041

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**Sent**: 9/4/2025 11:13:22 PM
**To**: Mellett, Timothy F (CRT) (b)(6)
**Subject**: RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields
**Attachments**: 2025.9.04 UT Privacy Letter.docx

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, September 4, 2025 4:21 PM
**To:** Bruzzone, Callie (CRT) <(b)(6)>; Wake, Brittany (CRT) <(b)(6)>
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

You can share: Yes, 52 U.S.C. § 21083(a)(2) Computerized list maintenance under both A and B; 52 U.S.C. § 21083(a)(5)(A) Requiring DL/SSN4

**(b)(5)**

You can share No, Privacy Act prohibits sharing with outside agencies. As would the data sharing agreement.

You can share CRA provides authority for last 22 months, but we have authority under NVRA and HAVA for these requests. 8(i) for NVRA and our enforcement authority. For HAVA, we cite the enforcement authority.

**From:** Bruzzone, Callie (CRT) <(b)(6)>
**Sent:** Thursday, September 4, 2025 4:15 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>; Wake, Brittany (CRT) <(b)(6)>
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Thank you – what of this information can I include in the letter?

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, September 4, 2025 3:49 PM
**To:** Bruzzone, Callie (CRT) <(b)(6)> Wake, Brittany (CRT) <(b)(6)>
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

See the answers in blue below.

**From:** Bruzzone, Callie (CRT) <(b)(6)>
**Sent:** Thursday, September 4, 2025 2:14 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>; Wake, Brittany (CRT) <(b)(6)>
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Tim,

I wanted to check in on this task, because it has become a bit more complicated than I expected. UT asks specific questions that are unaddressed in the TN model letter. I am not sure of the Section's position on some of these concerns. Here are the specific questions and what I know about each. Please let me know if my understanding is accurate and what to communicate to UT.

(b)(5)

(b)(5)

Thank you for your help with these questions.

Best,

Callie

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Wednesday, September 3, 2025 9:49 AM
**To:** Bruzzone, Callie (CRT) <(b)(6)>; Wake, Brittany (CRT) <(b)(6)>
**Subject:** FW: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Callie and Brittany,

See the attached correspondence from Utah. Please prepare a privacy letter for Utah using the letter to Tennessee as a model. Please send me a draft later today. Thanks,

Tim

---

**From:** Ryan Cowley (b)(6)
**Sent:** Friday, August 29, 2025 6:54 PM
**To:** Gates, Michael (CRT) (b)(6)
**Cc:** (b)(6)@utah.gov; Riordan, Maureen (CRT) (b)(6); Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** Re: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Mr. Gates, please find attached my response to your email dated August 22. 2025.

**Ryan Cowley** | **Director of Elections**
OFFICE OF LIEUTENANT GOVERNOR
DEIDRE M. HENDERSON
LTGOVERNOR.UTAH.GOV
801-538-1041

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

**From:** Bruzzone, Callie (CRT) [(b)(6)]
**Sent:** 9/4/2025 7:51:17 PM
**To:** Lott, Jasmin (CRT) [(b)(6)]; Rosenberg, Mary E. (CRT) (b)(6) Reid, Arielle (CRT) [(b)(6)]; Song, Harin C. (CRT) (b)(6)
**Subject:** FW: [EXTERNAL] Re: Complete Voter Registration List with All Fields

FYI

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Thursday, September 4, 2025 3:49 PM
**To:** Bruzzone, Callie (CRT) <(b)(6)>; Wake, Brittany (CRT) (b)(6)
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

See the answers in blue below.

**From:** Bruzzone, Callie (CRT) (b)(6)
**Sent:** Thursday, September 4, 2025 2:14 PM
**To:** Mellett, Timothy F (CRT) <(b)(6)>; Wake, Brittany (CRT) (b)(6)
**Subject:** RE: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Tim,

I wanted to check in on this task, because it has become a bit more complicated than I expected. UT asks specific questions that are unaddressed in the TN model letter. I am not sure of the Section's position on some of these concerns. Here are the specific questions and what I know about each. Please let me know if my understanding is accurate and what to communicate to UT.

(b)(5)

(b)(5) Yes, 52 U.S.C. § 21083(a)(2) Computerized list maintenance under both A and B; 52 U.S.C. § 21083(a)(5)(A) Requiring DL/SSN4

(b)(5)

(b)(5)

(b)(5) I think our general privacy act language and the offer of a data sharing agreement is a sufficient response here.
FYI, the data sharing agreement is not final yet. We are specifically doing searches and have an MOU with SSA for deceased voters. We don't see a need to send to DHS.

(b)(5)

(b)(5) Yes, VRL protected by Privacy Act. We also have cited the CRA.

(b)(5)

(b)(5) No, Privacy Act prohibits this. As would the data sharing agreement.

(b)(5)

(b)(5) Yes, SSA

(b)(5)

(b)(5) CRA provides authority for last 22 months, but we have authority under NVRA and HAVA for these requests. 8(i) for NVRA and our enforcement authority. For HAVA, we cite the enforcement authority.

Thank you for your help with these questions.

Best,

Callie

---

**From:** Mellett, Timothy F (CRT) <(b)(6)>
**Sent:** Wednesday, September 3, 2025 9:49 AM
**To:** Bruzzone, Callie (CRT) (b)(6) Wake, Brittany (CRT) (b)(6)
**Subject:** FW: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Hi Callie and Brittany,

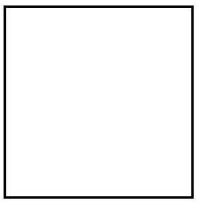
See the attached correspondence from Utah. Please prepare a privacy letter for Utah using the letter to Tennessee as a model. Please send me a draft later today. Thanks,

Tim

---

**From:** Ryan Cowley <(b)(6)>
**Sent:** Friday, August 29, 2025 6:54 PM
**To:** Gates, Michael (CRT) <(b)(6)>
**Cc:** (b)(6)@utah.gov; Riordan, Maureen (CRT) <(b)(6)>; Mellett, Timothy F (CRT) <(b)(6)>
**Subject:** Re: [EXTERNAL] Re: Complete Voter Registration List with All Fields

Mr. Gates, please find attached my response to your email dated August 22. 2025.



**Ryan Cowley** | Director of Elections
OFFICE OF LIEUTENANT GOVERNOR
DEIDRE M. HENDERSON
LTGOVERNOR.UTAH.GOV
801-538-1041

**From:** Osete, Jesus (CRT) (b)(6)
(b)(6)
**Sent:** 9/2/2025 10:28:47 PM
**To:** Gates, Michael (CRT) (b)(6)
**Subject:** RE: NASS call

Thanks. Can you please provide a recap of the R SOS meeting today when you get a chance?

**Jesus A. Osete**
Principal Deputy Assistant Attorney General
Civil Rights Division
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20579
(b)(6)
(b)(6)

**From:** Gates, Michael (CRT) (b)(6)
**Sent:** Sunday, August 31, 2025 7:17 PM
**To:** Osete, Jesus (CRT) <(b)(6)>
**Cc:** Mehr, Benjamin (OASG) <(b)(6)>
**Subject:** NASS call

Jesus, want to give you a recap of the call with National Association of Secretaries of State last Thursday – I had sent you and Ben the link to the meeting. The meeting was almost 30 minutes and about 7 or 8 questions were presented to me, some variations of the same basic question(s).

At open, Leslie announced that no media was welcome in the meeting, that it was only for Secretaries of State. She introduced me and allowed me to start off with a few comments about what we are doing and the meaning of our recent letters asking for Voter Registration Lists (VRLs). I stated that our aim is simply to fulfill our (AG) duties to enforce the NVRA and HAVA – particularly for list maintenance. I emphasized that we are here to help states test their lists, identify for areas that may require maintenance, and to provide that feedback to the states – all to be done discreetly and securely – outside of the view of the public.

Leslie asked the following questions, which I provided answers to:

1. Why is the DOJ doing this now?
    a. We have a duty to work with states to ensure that states have list maintenance programs and that the maintenance programs are working. It is a priority of this administration, and this Civil Rights Division, to ensure that the federal elections statutes are being followed. Historically, no administration or Civil Rights Division in previous administrations have really enforced these elections statutes (NVRA/HAVA). This is now a priority and our goal is to ensure compliance with federal law in advance of the 2026 elections.
2. What about PII, why do we need it?
    a. The more information we have for each voter (including DL or last 4SSN) the more reliable the VRL tests are going to be. The less information we have, the more error that will occur in our

list test results. It benefits both the DOJ (ensuring compliance) and the states that we are able to test VRLs and produce reliable results so that our feedback to states about their VRLs is reliable. Having the DL or the last 4SSN does that very thing – it ensures, or will prove, that the voters on the VRL are unique.

3. Is a state proving that they submit their VRL to ERIC enough to satisfy the DOJ?
    a. No because only the AG has the charge from Congress to ensure HAVA compliance – for instance, there is no private right of action under HAVA – only the AG can bring a HAVA action. We have a duty from Congress to ensure list maintenance and federal elections law compliance. We have to perform that duty. And, there is no way to verify that simply because a state has a contract with ERIC to submit data, does not mean that the VRLs are clean, free of ineligible voters, and NVRA/HAVA complaint.
4. Would the DOJ be willing to enter into MOU's with the states?
    a. Yes but the DOJ would present a standard MOU to those states – and the DOJ would not be negotiating 50 different MOUs that may consume months of time. If a state insists on an MOU, it will have to be entered into quickly and in a uniform way (the same or similar MOU presented to other states). I did make the point that the DOJ is primarily looking for name, address, DOB, and DL or last 4SSN and that most states already produce most of that information to any member of the public who requests a state's VRL pursuant to the NVRA. So, the MOU may be viewed as extra, unnecessary process to obtain largely the same information states are already producing as a public record.
5. What will be done with state's VRL data once we are done analyzing? Will the data go into a master voter database.
    a. The VRL data will be treated as information gathered pursuant to an investigation. It will be kept by the Civil Rights Division in accordance with records retention laws. Having said this, as VRLs are updated regularly with new voter registrations and more list maintenance by states, the VRLs sent to us won't be current for very long – with updates, they will become obsolete. So, there should be no concern for the DOJ's holding onto of the VRLs for the records retention period.

**Michael E. Gates**
Deputy Assistant Attorney General
Civil Rights Division
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
(b)(6)
(b)(6)

# National Voter Registration Act (NVRA)

## List maintenance investigations

Voting Section

U.S. Department of Justice
Civil Rights Division

# Overview

1. Summary of the NVRA
2. “Reasonable efforts” under the NVRA
3. The EAC’s EAVS report
4. Evaluating state responses
5. Preserving and protecting data and records

# Summary of the NVRA

## Summary of the National Voter Registration Act of 1993 (NVRA)

1. Signed into law on 5/20/1993, effective 1/1/1995
2. Enacted under the Elections Clause of the Constitution (Art. I, § 4, Cl. 1)
3. Requires states to register applicants that use a federal voter registration form, prohibits removal of registered voters from the voter rolls unless certain criteria are met, and **provides for list maintenance for federal elections**

## Exemptions from the NVRA (52 U.S.C. § 20503(b))

1. States that have continuously since 1/1/1994 not required voter registration for federal elections or offered election day registration for federal general elections are exempt
2. Six states are exempt: ***North Dakota***, which does not require registration, and ***Idaho***, ***Minnesota***, ***New Hampshire***, ***Wisconsin*** and ***Wyoming*** because they offer election day registration for federal general elections

## List maintenance under Section 8(a)(4) of the NVRA

> Each covered state is required to "conduct a general program that makes a **reasonable effort** to remove the names of ineligible voters from the official lists of eligible voters by reason of the death of the registrant; or a change in the residence of the registrant..."
>
> 52 U.S.C. § 20507(a)(4) (emphasis added)

# “Reasonable Efforts”

## List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Department's position:

> "[T]he question whether the general program of list maintenance [a state] undertakes in fact amounts to a 'reasonable effort' to remove ineligible voters under Section 8 of the NVRA goes beyond the simple existence of state laws and procedures, to include consideration of the actual efforts undertaken pursuant to those laws and procedures. Indeed, the NVRA requires states to '***conduct*** a general program that makes a reasonable effort to remove the names of ineligible voters.' 52 U.S.C. § 20507(a)(4) (emphasis added)."

## List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Department's position:

> "**States cannot meet this requirement merely by pointing to the existence of a state statute, regulation, or delegation. Indeed, there must be evidence that the state actually 'conduct[s]' the required 'general program**.' *Id.*; *see also*, *e.g.*, *Bellitto v. Snipes*, 935 F.3d 1192, 1205-07 (11th Cir. 2019) (considering whether jurisdiction's actual practices regarding removals for deaths amounted to reasonable effort to remove ineligible voters); *Missouri*, 535 F.3d at 850…"
>
> DOJ Statement of Interest, *PILF v. Boockvar* (E.D. Pa. Jan. 7, 2021)

## List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Illustrative definitions:

> "[A] state must establish a program that makes a **rational and sensible attempt to remove dead registrants**; a state need not, however, go to 'extravagant or excessive' lengths in creating and maintaining such a program."
>
> *Pub. Int. Legal Found. v. Benson*, No. 24-1255, 2025 WL 1300245, at *7 (6th Cir. May 6, 2025)

## List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Illustrative definitions:

> "[A] jurisdiction's reliance on reliable death records, such as **state health department records** and the **Social Security Death Index**, to identify and remove deceased voters constitutes a reasonable effort. The state is not required to exhaust all available methods for identifying deceased voters; it need only use reasonably reliable information to identify and remove such voters."
>
> *Bellitto v. Snipes*, 935 F.3d 1192, 1205 (11th Cir. 2019)

## List maintenance under Section 8(a)(4) of the NVRA: Safe harbor for states to comply with this requirement

> A state that uses Postal Service data from the **National Change of Address program (NCOA)** to identify voters who may have moved, sends those voters confirmation notices, and then removes voters who fail to respond to those notices and do not vote in the two subsequent federal general elections.
>
> 52 U.S.C. § 20507(c)(1); *see also Bellitto v. Snipes*, 935 F.3d 1192, 1195 (11th Cir. 2019) (calling it the "'**safe-harbor' provision**").

## List maintenance under Section 8(a)(4) of the NVRA: Safe harbor for states to comply with this requirement

> "Other possible examples of a general list maintenance program could include States undertaking a **uniform mailing** … to all voters in a jurisdiction, for which the State could use information obtained from returned non-deliverable mail" in place of NCOA data.
>
> Department of Justice, NVRA Questions & Answers ¶ 33, at http://www.justice.gov/crt/national-voter-registration-act-1993-nvra

13

# The EAVS Report and other data sources

## Data sources:
## Election Administration and Voting Survey (EAVS)

1. The U.S. Election Assistance Commission (EAC) compiles EAVS data on a biennial basis; the most recent data were released in June 2025
2. EAVS collects data on the number of voters dropped from registration rolls, the number of confirmation notices sent, and other list maintenance-related topics
3. Not all states provide complete data, which has required requesting the data directly from the states

# Data sources: Election Administration and Voting Survey (EAVS) – excerpt from 2022 report, pg. 188

## Voter Registration Table 5: Voter List Maintenance—Removal Actions

| State | Voters Removed | | Reason for Removal | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Reg. Voters | Moved Out of Jurisdiction | | Voter Deceased | | Failure to Return Confirmation Notice | | Voter's Request | |
| | | | Total | % | Total | % | Total | % | Total | % |
| Alabama [1] | 298,554 | 8.1% | 20,019 | 6.7% | 106,738 | 35.8% | 149,982 | 50.2% | 833 | 0.3% |
| Alaska | 46,703 | 7.2% | 2,683 | 5.7% | 11,261 | 24.1% | 22,937 | 49.1% | 8,400 | 18.0% |
| American Samoa | 2,736 | 19.1% | – | – | 146 | 5.3% | 2,590 | 94.7% | – | – |
| Arizona | 432,498 | 8.9% | 81,637 | 18.9% | 108,103 | 25.0% | 175,284 | 40.5% | 50,092 | 11.6% |
| Arkansas | 195,595 | 10.8% | 10,598 | 5.4% | 46,867 | 24.0% | 128,798 | 65.8% | 692 | 0.4% |
| California | 977,773 | 3.6% | 167,009 | 17.1% | 406,702 | 41.6% | 155,399 | 15.9% | 137,839 | 14.1% |
| Colorado | 394,628 | 9.1% | 59,977 | 15.2% | 99,024 | 25.1% | 161,607 | 41.0% | 64,478 | 16.3% |

# Data sources: Election Administration and Voting Survey (EAVS) – excerpt from 2022 report, pg. 190

| State | Reason for Removal | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Felony or Conviction | | Mental Incompetence | | Other | | Not Categorized | |
| | Total | % | Total | % | Total | % | Total | % |
| Alabama [1] | 5,815 | 1.9% | 145 | 0.0% | 13,870 | 4.6% | 1,152 | 0.4% |
| Alaska | 1,422 | 3.0% | 0 | 0.0% | – | – | 0 | 0.0% |
| American Samoa | 0 | 0.0% | – | – | – | – | 0 | 0.0% |
| Arizona | 15,172 | 3.5% | 717 | 0.2% | 1,493 | 0.3% | 0 | 0.0% |
| Arkansas | 3,391 | 1.7% | 57 | 0.0% | 5,192 | 2.7% | 0 | 0.0% |
| California | 18,657 | 1.9% | 980 | 0.1% | 53,166 | 5.4% | 38,021 | 3.9% |
| Colorado | 9,480 | 2.4% | – | – | 62 | 0.0% | 0 | 0.0% |

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

## Preserving and protecting data and records: The Privacy Act

1. Personally Identifiable Information (PII) in voter records must be protected
2. Includes the following limitations:
   - CRT/VOT may collect only data it is authorized to collect
   - Access to data is limited to only those who need access for their assigned work
   - Data is accessible in the secured files are user/password limited

## Preserving and protecting data and records:
## Records and Information Management (RIM)

Everyone is required to read and comply with CRT's RIM policy in:

1. Creating records and documenting activities for which you are responsible
2. Preserving records in a secure and efficient manner
3. Maintaining records according to CRT's RIM policy
4. Ensuring disposition of records comply with CRT's RIM policy and federal law

# Discussion and Questions

U.S. Department of Justice
Civil Rights Division

**DOCUMENT WITHHELD IN FULL UNDER FOIA EXEMPTION B(5).**

# National Voter Registration Act (NVRA)

## List maintenance investigations

Voting Section

U.S. Department of Justice
Civil Rights Division

# Overview

1. Summary of the NVRA
2. “Reasonable efforts” under the NVRA
3. The EAC’s EAVS report
4. Evaluating state responses
5. Preserving and protecting data and records

# Summary of the NVRA

# Summary of the National Voter Registration Act of 1993 (NVRA)

1. Signed into law on 5/20/1993, effective 1/1/1995
2. Enacted under the Elections Clause of the Constitution (Art. I, § 4, Cl. 1)
3. Requires states to register applicants that use a federal voter registration form, prohibits removal of registered voters from the voter rolls unless certain criteria are met, and **provides for list maintenance for federal elections**

# Exemptions from the NVRA (52 U.S.C. § 20503(b))

1. States that have continuously since 1/1/1994 not required voter registration for federal elections or offered election day registration for federal general elections are exempt
2. Six states are exempt: ***North Dakota***, which does not require registration, and ***Idaho***, ***Minnesota***, ***New Hampshire***, ***Wisconsin*** and ***Wyoming*** because they offer election day registration for federal general elections

# List maintenance under Section 8(a)(4) of the NVRA

Each covered state is required to "conduct a general program that makes a **reasonable effort** to remove the names of ineligible voters from the official lists of eligible voters by reason of the death of the registrant; or a change in the residence of the registrant..."

52 U.S.C. § 20507(a)(4) (emphasis added)

# “Reasonable Efforts”

# List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Department's position:

> "[T]he question whether the general program of list maintenance [a state] undertakes in fact amounts to a 'reasonable effort' to remove ineligible voters under Section 8 of the NVRA goes beyond the simple existence of state laws and procedures, to include consideration of the actual efforts undertaken pursuant to those laws and procedures. Indeed, the NVRA requires states to '***conduct*** a general program that makes a reasonable effort to remove the names of ineligible voters.' 52 U.S.C. § 20507(a)(4) (emphasis added)."

# List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Department's position:

"**States cannot meet this requirement merely by pointing to the existence of a state statute, regulation, or delegation. Indeed, there must be evidence that the state actually 'conduct[s]' the required 'general program**.' *Id.*; *see also*, *e.g.*, *Bellitto v. Snipes*, 935 F.3d 1192, 1205-07 (11th Cir. 2019) (considering whether jurisdiction's actual practices regarding removals for deaths amounted to reasonable effort to remove ineligible voters); *Missouri*, 535 F.3d at 850…"

DOJ Statement of Interest, *PILF v. Boockvar* (E.D. Pa. Jan. 7, 2021)

# List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Illustrative definitions:

> "[A] state must establish a program that makes a **rational and sensible attempt to remove dead registrants**; a state need not, however, go to 'extravagant or excessive' lengths in creating and maintaining such a program."
>
> *Pub. Int. Legal Found. v. Benson*, No. 24-1255, 2025 WL 1300245, at *7 (6th Cir. May 6, 2025)

# List maintenance under Section 8(a)(4) of the NVRA: What is a "reasonable effort"? Illustrative definitions:

"[A] jurisdiction's reliance on reliable death records, such as **state health department records** and the **Social Security Death Index**, to identify and remove deceased voters constitutes a reasonable effort. The state is not required to exhaust all available methods for identifying deceased voters; it need only use reasonably reliable information to identify and remove such voters."

*Bellitto v. Snipes*, 935 F.3d 1192, 1205 (11th Cir. 2019)

# List maintenance under Section 8(a)(4) of the NVRA: Safe harbor for states to comply with this requirement

> A state that uses Postal Service data from the **National Change of Address program (NCOA)** to identify voters who may have moved, sends those voters confirmation notices, and then removes voters who fail to respond to those notices and do not vote in the two subsequent federal general elections.
>
> 52 U.S.C. § 20507(c)(1); *see also Bellitto v. Snipes*, 935 F.3d 1192, 1195 (11th Cir. 2019) (calling it the "'**safe-harbor' provision**").

# List maintenance under Section 8(a)(4) of the NVRA: Safe harbor for states to comply with this requirement

> "Other possible examples of a general list maintenance program could include States undertaking a **uniform mailing** … to all voters in a jurisdiction, for which the State could use information obtained from returned non-deliverable mail" in place of NCOA data.
>
> Department of Justice, NVRA Questions & Answers ¶ 33, at http://www.justice.gov/crt/national-voter-registration-act-1993-nvra

# The EAVS Report and other data sources

# Data sources:
# Election Administration and Voting Survey (EAVS)

1. The U.S. Election Assistance Commission (EAC) compiles EAVS data on a biennial basis; the most recent data were released in June 2025
2. EAVS collects data on the number of voters dropped from registration rolls, the number of confirmation notices sent, and other list maintenance-related topics
3. Not all states provide complete data, which has required requesting the data directly from the states

# Data sources: Election Administration and Voting Survey (EAVS) – excerpt from 2022 report, pg. 188

## Voter Registration Table 5: Voter List Maintenance—Removal Actions

| State | Voters Removed | | Reason for Removal | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Reg. Voters | Moved Out of Jurisdiction | | Voter Deceased | | Failure to Return Confirmation Notice | | Voter's Request | |
| | | | Total | % | Total | % | Total | % | Total | % |
| Alabama [1] | 298,554 | 8.1% | 20,019 | 6.7% | 106,738 | 35.8% | 149,982 | 50.2% | 833 | 0.3% |
| Alaska | 46,703 | 7.2% | 2,683 | 5.7% | 11,261 | 24.1% | 22,937 | 49.1% | 8,400 | 18.0% |
| American Samoa | 2,736 | 19.1% | – | – | 146 | 5.3% | 2,590 | 94.7% | – | – |
| Arizona | 432,498 | 8.9% | 81,637 | 18.9% | 108,103 | 25.0% | 175,284 | 40.5% | 50,092 | 11.6% |
| Arkansas | 195,595 | 10.8% | 10,598 | 5.4% | 46,867 | 24.0% | 128,798 | 65.8% | 692 | 0.4% |
| California | 977,773 | 3.6% | 167,009 | 17.1% | 406,702 | 41.6% | 155,399 | 15.9% | 137,839 | 14.1% |
| Colorado | 394,628 | 9.1% | 59,977 | 15.2% | 99,024 | 25.1% | 161,607 | 41.0% | 64,478 | 16.3% |

# Data sources: Election Administration and Voting Survey (EAVS) – excerpt from 2022 report, pg. 190

| State | Reason for Removal | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Felony or Conviction | | Mental Incompetence | | Other | | Not Categorized | |
| | Total | % | Total | % | Total | % | Total | % |
| Alabama [1] | 5,815 | 1.9% | 145 | 0.0% | 13,870 | 4.6% | 1,152 | 0.4% |
| Alaska | 1,422 | 3.0% | 0 | 0.0% | – | – | 0 | 0.0% |
| American Samoa | 0 | 0.0% | – | – | – | – | 0 | 0.0% |
| Arizona | 15,172 | 3.5% | 717 | 0.2% | 1,493 | 0.3% | 0 | 0.0% |
| Arkansas | 3,391 | 1.7% | 57 | 0.0% | 5,192 | 2.7% | 0 | 0.0% |
| California | 18,657 | 1.9% | 980 | 0.1% | 53,166 | 5.4% | 38,021 | 3.9% |
| Colorado | 9,480 | 2.4% | – | – | 62 | 0.0% | 0 | 0.0% |

(b)(5)

(b)(5)

(b)(5)

# Status Update

# Evaluating state responses:

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

# Preserving and protecting data and records:
## The Privacy Act

1. Personally Identifiable Information (PII) in voter records must be protected
2. Includes the following limitations:
   - CRT/VOT may collect only data it is authorized to collect
   - Access to data is limited to only those who need access for their assigned work
   - Data is accessible in the secured files are user/password limited

# Preserving and protecting data and records:
# Records and Information Management (RIM)

Everyone is required to read and comply with CRT's RIM policy in:

1. Creating records and documenting activities for which you are responsible
2. Preserving records in a secure and efficient manner
3. Maintaining records according to CRT's RIM policy
4. Ensuring disposition of records comply with CRT's RIM policy and federal law

# Discussion and Questions

U.S. Department of Justice
Civil Rights Division