



USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”
03/19/2025	1.1	CasePoint Staff converted PIA data to new template

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project	3
Mission Area System/Program Contacts	3
Abstract	4
Overview	4
Section 1: Authorities and Other Requirements	6
Section 2: Characterization of the Information	7
Section 3: Uses of the Information	10
Section 4: Notice	11
Section 5: Data Retention	12
Section 6: Information Sharing.....	13
Section 7: Redress	15
Section 8: Auditing and Accountability	17

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	MRP CasePoint (MRPCP)
Program Office	eDiscovery
Mission Area	MRP/APHIS
CSAM Number	2629
Date Submitted for Review	TBD

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Angela Cole	202-465-6265
Information System Security Manager	Alice Strickland	301-377-1329
System/Program Managers	Thomas Welsch	305-202-4157

Abstract

CasePoint is a secure cloud electronic discovery (eDiscovery) platform that allows the USDA's Animal and Plant Health Inspection Service (APHIS) to process records for litigation, investigations, and Freedom of Information Act (FOIA) requests. CasePoint serves as a document processing tool that supports the organization of digitized hardcopy and electronic documents for analysis, review, redaction, and production to meet litigation discovery and FOIA requirements. This PIA is being conducted because CasePoint stores the personally identifiable information (PII) of individuals who are involved in or subject to litigations, investigations or FOIA requests. It should be noted that CasePoint does not collect any PII directly from individuals, but instead collects documents, emails and other electronic artifacts that may contain PII from other USDA source systems.

Overview

CasePoint is a full-spectrum eDiscovery platform that is used to assist APHIS with managing electronically stored information and scanned hardcopy documents used for discovery in litigation matters, investigations, and Freedom of Information Act (FOIA) requests. eDiscovery refers to discovery in legal proceedings such as litigation, government investigations, or FOIA requests, where the information sought is in electronic format. CasePoint assists APHIS with the management of large volumes of records used in support of these requests. With CasePoint, the USDA can complete discovery projects efficiently and with greater accuracy using a single, integrated, and easy-to-use tool.

Electronic information collected in CasePoint may include, but is not limited to, emails, text messages, spreadsheets, PowerPoints, word documents, digital photographs, audio and visual recordings and voicemails. The content and metadata (information associated with the content) of these electronic information types may include the PII of individuals. APHIS eDiscovery works on cases within APHIS's purview such as Freedom of Information Act requests, administrative records cases for APHIS litigations, and public comments cases on regulation proposals. This means that members of the public with whom the USDA interacts and any APHIS staff who they interact with via email can be present in data provided to CasePoint.

Once electronic information has been retrieved by source systems, the records must be secured and preserved in a legally defensible manner. A critical element of eDiscovery is to avoid alteration and deletion of these documents. CasePoint preserves the integrity of the uploaded content and ensures all the metadata is maintained in its original format and that key attributes are retained.

Authorized users may upload copies of any type of file from any source. Most commonly, records in the system consist of emails with their attachments compiled after an automated search. Users may also include documents located following manual searches of shared drives, SharePoint sites, OneDrive, and other source systems. All these records are manually uploaded to CasePoint. There are no direct interconnections with any systems or storage areas. Raw data, referred to here as "records", can come from any electronic source, to include Microsoft Purview collections, EnCase file share/workstation collections and self-collection performed by requestors and handed over to the eDiscovery team.

Limited APHIS employees upload electronic documents in CasePoint to create a new “case.” Records in CasePoint are segregated by case and subcase. The APHIS eDiscovery program staff manually grant access privileges to attorneys, paralegals, and other support analysts assigned to that matter, allowing them to access and review the documents. Only internal APHIS users with valid need-to-access are granted access to a case or sub-case by the system administrator. This includes attorneys and FOIA analysts assigned to a particular case, and agency staff reviewing documents for a case.

APHIS primarily uses CasePoint to review large volumes of documents to determine what is relevant to a matter. Users may access the system to view their case data and perform actions through menus to further filter, cull, and manage the data. This allows users to gather and prepare the case file for review. CasePoint allows authorized users to also:

- Place documents in folders
- Add tags to documents
- Search
- Batch documents for review
- Convert documents from native formats to PDF
- Index documents
- Apply redactions

CasePoint supports the processing and analysis activities involved in reviewing and preparing cases for review by the attorneys on the case. It has built-in tools to help automatically find relevant information related to cases, and to reduce redundant and duplicate information. Only authorized users with appropriate access rights may access, review, and remove the data. CasePoint handles approximately 360 cases per year.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

What legal authorities and/or agreements permit the collection of information by the project or system?

The authority to compile documents is governed by the Federal Rules of Civil Procedure (28 USC Appendix), the Freedom of Information Act (5 USC § 552), Administrative Procedure Act (5 USC §551 et seq.).

CasePoint is an ediscovery tool that supports litigation, FOIA, and investigations (all legal authorities) by accessing APHIS systems only on an as needed basis. It does not continuously collect or store PII, nor does it gather information from the public; instead, it ingests records solely when a specific case requires discovery. Content in CasePoint comes from other systems of record. There is no original collection of information done through CasePoint. The governing authorities for the original collections of information are dependent on the functional authority of the office originally collecting the information.

Has Authorization and Accreditation (A&A) been completed for the system?

Yes, this system received an Authority to Operate on June 22, 2023, and is valid until June 22, 2026. The System Security Plan is updated annually (latest update was in June 2024). The annual assessment began in July 2024. CasePoint is categorized as a Moderate System in accordance with the Federal Information Processing Standard (FIPS) 199.

What System of Records Notice(s) (SORN(s)) apply to the information?

All information in CasePoint originally comes from other source systems and is covered under the SORNs of the original collection. OMB Circular A-108, Section 6, requires agencies to publish SORNs for the systems of records they maintain. CasePoint is not a system of records; it is a **discovery tool**. The applicable SORN always belongs to the source APHIS system where the records originate.

Is the collection of information covered by the Paperwork Reduction Act?

No.

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

What information is collected, used, disseminated, or maintained in the system/program?

Identifying Numbers

- Social Security Number
- Truncated or Partial Security Number
- Driver's License number
- Registration number
- File/Case ID number
- Student ID number
- Employee Identification number
- Professional License number
- Taxpayer Identification number
- Business Taxpayer Identification number (sole proprietor)
- Personal Bank Account number
- Personal Mobile number
- Business Mobile number (sole proprietor)

Biographical Information

- Name (Including Nicknames)
- Business Mailing Address (sole proprietor)
- Date of Birth (MM/DD/YY)
- Business Phone or Fax Number (sole proprietor)
- Home Address
- ZIP Code
- Personal Email Address
- Business Email Address
- Employment Information
- Education Information
- Business Financial Information (Including loan information)

Distinguishing Features

- Signatures
- Photos

Characteristics

- Voice/Audio Recording

Specific Information/File Types

- Case Files

What are the sources of the information in the system/program?

CasePoint may store copies of data from any APHIS source system. Records in CasePoint may originate from formal or informal source systems or any paper documents scanned into an electronic format for review. The information in the system mainly comes from Microsoft Outlook in Office 365 but may come from any other APHIS system. Raw data, referred to here as “records”, can come from any electronic source, to include Microsoft Purview collections, EnCase file share/workstation collections and self-collections performed by requestors and handed over to the eDiscovery team.

How is the information collected?

All records are manually uploaded to CasePoint by members of the e-Discovery team. There are no direct connections with any systems or storage areas. The information is not collected but rather a by-product of performing eDiscovery activities. eDiscovery entails searching for, compiling, and reviewing records responsive to a request. Searchers seek materials from a variety of locations using manual and automatic processes. Hardcopy records may be scanned. This content is then uploaded to CasePoint for review.

Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

The system does not use commercial or publicly available data.

How will the information be checked for accuracy? How often will it be checked?

The overall accuracy of the records is dependent on the origin system of record. Records are not altered after ingesting into CasePoint to ensure the integrity of the discovery process.

Does the system/program use third-party websites?

No

What is the purpose of the use of third-party websites?

N/A The system does not use third-party websites.

What PII will be made available to the agency though the use of third-party websites?

N/A The system does not use third-party websites.

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: Due to the nature of e-discovery and the need to pull all relevant information related to a case, there can be a wide range of PII pulled into CasePoint, including sensitive PII such as Social Security Numbers. There is also a privacy risk that CasePoint may maintain more information than necessary resulting in the overcollection of data within the system. Because the e-Discovery process requires that information not be altered in any way to protect the integrity of the judicial process, inaccuracies of data in CasePoint must be maintained and cannot be corrected. Therefore, some information may be inaccurate.

Mitigation: CasePoint only collects information when it is under a legal mandate to respond to discovery and other document requests. Search coordinators and searchers will strive to narrow the scope and search strategies to the greatest extent possible to limit the volume of content that is uploaded to CasePoint, which is a requirement of their formal e-Discovery processes and standards. Once data has been uploaded to CasePoint, there are additional search strategies that help in finding relevant information and reducing redundant information or information that is not relevant to the case. These include proximity searches (searching two separate search terms at the same time that are also within a certain number of words of each other), stemming searches (searches that use the root of a word such as “search” to return results that would include “searches, “searched”, “searching”, as well as “search”), and exclusionary searches that avoid items known not to be relevant such as broadcast emails from the USDA or sales and marketing emails, etc. These additional search strategies are employed by AHPIS eDiscovery personnel on behalf of requestors.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

CasePoint is an eDiscovery platform that allows APHIS to process records for litigation, investigations, and FOIA requests. CasePoint allows the e-Discovery team to organize digitized hardcopy and electronic documents for analysis, review, redaction, and production to meet litigation discovery and FOIA requests in an efficient manner. All the PII in the system is used to serve as official records and evidence related to litigations, investigations and FOIA requests.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

The integration of Artificial Intelligence (AI) and analytics is an integral part of CasePoint. Through AI-powered technology, CasePoint efficiently reviews, identifies, and prioritizes the most relevant documents related to a case or request. The AI tools are not used to discover or locate a predictive pattern or an anomaly about individuals. They are only used to help find documents that are relevant to cases and help reduce duplicated documents.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: There is a privacy risk that information in CasePoint will be used outside of its intended purpose of gathering electronic documents as part of eDiscovery or FOIA requests.

Mitigation: APHIS manages its own private instance of CasePoint. The only time that information is uploaded into CasePoint would be in response to litigation, FOIA, or investigative matters. Access to the system requires supervisor and system owner approval and is documented on the APHIS User Account Control Form. The application limits access to relevant information through assigned user roles, which enforce need-to-know and least privilege concepts, which ensure that users only have access to information that they need to carry out their job responsibilities. Cases are partitioned to ensure only assigned users have access to files related to their cases. The batching within cases further limits access to authorized individuals. Auditing is enabled at the database and web application level which creates logs that detail objects accessed by users. These logs are automatically generated by CasePoint and are reviewed by CasePoint Administrators when there is evidence or reason to believe that the integrity of the data has been compromised.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

How does the project/program/system provide notice to individuals prior to collection?

CasePoint is not the original point of collection of information from individuals. Electronic information is derived from the system of origin, and it is therefore incumbent on the systems that originally collected the data to provide notice to individuals. However, APHIS does provide general notice through this PIA that electronic information may be stored in CasePoint for eDiscovery purposes.

What options are available for individuals to consent, decline, or opt out of the project?

CasePoint does not collect PII directly from the individual. Any right or opportunity to consent or decline to provide information occurs at the point of original collection from the individual and is described in the relevant PIA and SORN for that system of origin.

Privacy Impact Analysis: Related to notice.

Privacy Risk: There is a privacy risk that individuals are not aware their records are transferred to CasePoint for eDiscovery purposes.

Mitigation: CasePoint does not collect PII directly from the data subject and relies on source systems to provide notice to the individual prior to collection of information. APHIS is publishing this PIA to serve as notice of CasePoint, the data it collects and maintains, and the limited purposes for which APHIS uses the data.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

What information is retained and for how long?

Once the e-Discovery process is complete, the information related to a case in CasePoint is downloaded to a secure local server where it is shared with the relevant parties, such as FOIA or legal teams that are handling the case (please see questions about internal and external sharing in this PIA for details). A case is closed in CasePoint when relevant materials are identified and presented to authorized parties, and it is confirmed that no further need for e-discovery is anticipated (e.g. for appeals). At that point, the information in CasePoint is deleted. The exported files on the secure local server are retained for three years as part of the e-Discovery team's internal policy.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

The records in CasePoint are considered convenient copies of the information and are not subject to NARA retention schedules. The versions of the information that are formally subject to NARA retention schedules are managed in the original source systems, and by the team that receives the exported copies from CasePoint (generally FOIA or legal teams that are managing the cases). CasePoint is used only as a tool for temporarily gathering and organizing information.

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: Retaining information that is not subject to NARA retention increases the risk of unauthorized access or disclosure the longer it is maintained.

Mitigation: All documents pertaining to a case are deleted in CasePoint immediately after the case is closed and it is determined that there will be no further need for e-discovery. The exported case files are stored on the secure local server for three years after this time, a period which balances the potential practical need for access to these files after a case is closed with the privacy interests and protection of information of the individuals whose PII is contained in the files. Access to these archived files is limited to the eDiscovery team only.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

The information in CasePoint is shared with internal components involved in eDiscovery, which varies based on the case but generally includes the APHIS FOIA office, USDA Office of the Inspector General, and USDA Office of General Counsel. Within APHIS, the data is shared by providing the recipient with access to the folder on the secure local server that contains the case files that have been exported from CasePoint. Only the specific individuals who require access are provided with it, and they are only provided with access to the specific case that they are working on. When data is shared within the USDA but outside of APHIS, the case files are uploaded to a FedRAMP (Federal Risk and Authorization Management Program) Box account, and the recipient is provided with a link to access and download the files from the Box folder. Only the recipient who requires access is provided with it, and they only have access to the case file that they are working on. The case files are deleted in Box by the e-Discovery team 14 days after sharing as part of their standard business process.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: There is a risk of unauthorized access or sharing of data while the case files are being transmitted internally.

Mitigation: To reduce this risk, permission to access the case files on the secure local server and Box that are used for internal sharing are granted only to those who have an official need-to-know. The two members of the e-Discovery team are the sole administrators for these two repositories. Access is reviewed for every new case to ensure proper access is assigned to review specific delivery paths.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

The case files in CasePoint may be shared with the U.S. Department of Justice in support of litigation. In these instances, the case files are uploaded to a FedRAMP Box folder, and the recipient is provided with a link to access and download the files from the Box folder. Only the recipient who requires access is provided with it, and they only have access to the case file that they are working on. The case files are deleted in Box by the e-Discovery team 14 days after sharing as part of their standard business process.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: Risks associated with external sharing include the possibility of the data being accessed by unauthorized personnel.

Mitigation: A folder in box, named by court case, is used for each case that is shared externally, and access is only provided to recipients who require it. There are two e-Discovery administrators that have access to the administrative side of the FedRAMP Box account, and they are responsible for providing access via Box. As part of the e-Discovery team's standard business process, access to the Box folders for external recipients is deleted 14 days after access is granted to further reduce the risk of unauthorized access to the case files.

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

What are the procedures that allow individuals to gain access to their information?

Individuals are not able to access their information directly in CasePoint due to its role in the discovery process. Individuals seeking access to their records follow the procedures for the source system or source data.

Individuals seeking access to his or her records in any of the source systems may file a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person may file a FOIA request. USDA offers several avenues to request access to their records. Individuals may file a Privacy Act request to view their record by submitting a Privacy Act request online through USDA's Public Access Link (PAL), or through mail or fax.

- USDA – Animal and Plant Health Inspection Service
- FOIA and Privacy Act Director
- 5601 Sunnyside Avenue
- Beltsville, MD 20705
- Facsimile: 301-734-5941
- Email: APHISPrivacy@usda.gov

Further information about Privacy Act and FOIA requests for APHIS records is available at [Freedom of Information Act home page](#)

What are the procedures for correcting inaccurate or erroneous information?

APHIS has an obligation to preserve records in its original form and take reasonable steps to maintain the integrity of the record as part of the e-Discovery process. The data in CasePoint must be maintained in its original form for legal analysis. There are no procedures for individuals to correct erroneous information while records are under eDiscovery review. USDA must take reasonable steps to ensure that the electronically stored information in CasePoint is not altered or destroyed in any way.

Individuals may address any inaccuracies or errors within the system of origin by filing a Privacy Act request to the FOIA Officer as described in Section 7.1.

How are individuals notified of the procedures for correcting their information?

The APHIS FOIA webpage and this PIA inform individuals on the general procedures for correcting records. There are no specific notifications on procedures on how to correct records in CasePoint, since this is not possible. Updating records in CasePoint would run counter to discovery, FOIA, and investigatory requirements.

If no formal redress is provided, what alternatives are available to the individual?

APHIS offers a formal redress process to access and correct records from the source systems.

Privacy Impact Analysis: Related to redress.

Privacy Risk: Users are not able to access or update their information in CasePoint, thereby limiting their rights to redress.

Mitigation: The USDA is not able to fully mitigate this risk, as the purpose of eDiscovery is to support the mandatory production of records in pending litigation. Federal disclosure laws (specifically Federal Rules of Civil Procedure (Rule 34 1 (a) - Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes as well as Rule 26 Subdivision (b)(2) Duty to Disclose; General Provisions Governing Discovery) require production of documents in their original form, even if they contain erroneous, incomplete, or outdated information. Incorrect information can be corrected in the source system. However, active litigation may prevent the correction of the information if it alters the original record (i.e., rather than creating a separate updated record) because federal disclosure laws require production of documents in their original form, which must be maintained throughout the litigation. Throughout the eDiscovery process, the USDA must take reasonable steps to ensure that the chain of custody is maintained and that the electronic information in CasePoint is not altered or destroyed. However, the USDA does provide the opportunity for individuals to submit requests to access or update their information in the source systems and depending on the type of request or status of a case or investigation, the request may be granted.

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

How is the information in the system/project/program secured?

- All access to the system is limited to USDA APHIS employees/contractors and enforced via multi-factor log-in credentials, which requires users to provide an additional form of authentication beyond their password. Access is also regularly audited.
- The application limits access to relevant information through assigned user roles, which enforce need-to-know and least privilege concepts, ensuring that individuals only have access to information that they need to carry out their work.
- The partitioning of datasets ensures that programs only have access to files related to their cases.
- The batching within cases further limits access to authorized individuals.
- User actions can be logged to understand who made changes to information in cases of misuse of data.
- All information in the system is secured with encryption, which ensures that information will remain unreadable to unauthorized users.
- The storage server where case files from CasePoint are exported is administered by the eDiscovery team. Landing path access is only granted to requestors when they have data to land for their specific case. Delivery paths are locked to the eDiscovery team and those designated by the requestor to be recipients of their productions.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

Initial requests for granting access to CasePoint are routed from the user through their supervisor to the system owner. Need-to-know determinations are made at both the supervisor and system owner level. If validated, the request is passed on to the system administrator. The user and system owner are notified via email that the request has been processed along with instructions for the initial login. User profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual's access will be disabled, and the same procedures as noted above must be completed to renew access. All access to CasePoint is authorized and documented by APHIS Form 513, APHIS User Account Control Form. APHIS Form 513s for access to CasePoint are contained within the User Management System (UMS).

Granting access to the folders on the secure server and in Box that are used for sharing case files is completed by the e-Discover administrators. Once they confirm that the recipient has a legitimate need for the case files, they provide access to the individual to a folder that contains only the case files they are authorized to access. All access procedures for CasePoint, the secure file server and Box are documented in the unit's standard operating procedures.

How does the program review and approve information sharing requirements?

Information in CasePoint is only shared to meet litigation, discovery, and FOIA requirements. The e-Discovery Program Coordinator is responsible for reviewing and approving any information sharing requests.

Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

APHIS requires all system users to complete annual USDA information security awareness training that includes a section dedicated to privacy. Each user must read and sign the accompanying rules of behavior prior to receiving access to the information system. Failure to complete the mandatory training results in APHIS terminating system access.