U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Security and Hazardous Materials Safety (ASH)
Cyber Analysis Virtual Environment (CAVE)

Responsible Official

Atul Celly
Email: Atul.Celly@faa.gov
Phone Number: 202-267-5662

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration (FAA) Office of Security and Hazardous Materials Safety (ASH) Office of Investigations (AXI) uses the Cyber Analytics Virtual Environment (CAVE) for three main programs: Cyber Investigations, electronic discovery (eDiscovery), and unmanned aircraft system (UAS) digital storage investigations. AXI investigators use CAVE tools to collect digital evidentiary data from FAA employees, contractors, and members of the public. The data collected is used to support civil, administrative, criminal, and other investigative or discoverable matters such as a Freedom of Information Act (FOIA) case, litigation, or Congressional requests. The system operates under the following authorities: Title 49 United States Code (U.S.C.), chapter 449, *Air Transportation Security*, enacted as Pub. L. 103–272 on July 5, 1994; *Transportation Safety Act of 1974*; *FAA Drug Enforcement Assistance Act of 1988*; Executive Order (E.O.), 10450, *Security Requirements for Government Employment*; E.O. 12968, *Access to Classified Information*; and E.O. 12829, *National Industrial Security Program*.

The FAA is publishing this Privacy Impact Assessment (PIA) for the CAVE in accordance with Section 208 of the E-Government Act of 2002 because the system processes Personally Identifiable Information (PII) from members of the public including individuals that are associated with an FAA employee or contractor who is the subject of an investigation, and UAS operators associated with an investigation or whose information is contained on a seized UAS.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Federal Aviation Administration (FAA) Office of Security and Hazardous Materials Safety (ASH) Office of Investigations (AXI) uses CAVE to support FAA investigations. AXI's Technical Investigations Division uses CAVE for Cyber Investigations, eDiscovery, and unmanned aircraft system (UAS) digital storage investigations programs. Before the development of CAVE these functions were dispersed throughout the FAA. The creation of CAVE allows for managing all these separate functionalities under one system which has resulted in greater efficiency and security by managing related data under one system. The FAA AXI Technical Investigations Division uses CAVE to conduct cyber investigations of administrative, insider threat, defensive counterintelligence, and other investigations of the FAA, UAS forensics, and e-Discovery. AXI uses CAVE to collect digital evidentiary data from FAA employees, contractors, and members of the public (individuals associated with an investigation of a FAA employee/contractor). The data collected is used to support civil, administrative, criminal, and other investigative or discoverable matters such as FOIA cases, litigation, or Congressional requests.

Cyber Investigations:

The first function supported by CAVE is cyber investigations. The FAA relies on AXI's Cyber Investigations team to support civil, administrative, criminal, and other investigative requests. AXI cyber investigators use tools in CAVE to remotely access the FAA employee or contractor's computer to collect digital evidentiary data. An investigation begins when a

Cyber Investigations team member, also known as Cyber Forensic Investigator (CFI), receives a request to conduct a review and analysis of data, which can include an FAA employee/contractor name, address, phone number, Internet Protocol (IP) address, computer hostname, and/or user identification (ID). A cyber investigations case is then opened and assigned a case number in the Investigative Tracking System (ITS). ITS is the Office of Investigations management system which is separate from and not connected to CAVE.

The CFI then remotely accesses the FAA employee or contractor's system and/or equipment to collect data according to the request of the investigation. This is done without the FAA employee or contractor's knowledge. Collected data may include email, virtual private network (VPN) logs, data residing on network servers, keystroke data, FAA-issued mobile device data, publicly available websites, and logs from the FAA Security Operations Center (SOC) that are within the scope of the request. An AXI CFI may use the Keystroke Capture feature deployed to an FAA workstation that is the subject of an investigation. The Keystroke Capture tool records and identifies what is being typed on FAA employee or contractor's computer keyboard. This tool is only used when there is a specific requirement based on the scope of the investigation and includes a specific timeframe for the data capture. Any use of the Keystroke Capture tool must be approved by an AXI Branch Manager, Deputy Director, or Director for a specified timeframe and specified FAA employee or contractor's computer/system. Additionally, the Keystroke Capture feature may only be used when there is a specific requirement based on the scope of the investigation and it has been determined that relevant data pertinent to the investigation cannot be obtained in another way.

The CFI may also use the Screen Capture feature deployed to an FAA workstation belonging to an FAA employee or contractor who is the subject of an investigation. The Screen Capture tool records incremental screenshots of a remote FAA employee or contractor's computer desktop display based on a specific event that is determined by the scope of the investigation and includes the length of time the tool is active and what events are to be captured. The Screen Capture feature records and sends the screenshots of the workstation's desktop display in real-time logs which are exported to a CFI's forensic workstation for review and analysis. The deployment and activation of the Screen Capture feature must be approved by the AXI management to include the length of time the tool is active and what events are to be captured.

The CFI then uses the Magnet AXIOM tool to process the collected data, analyze it, and identify if any of the collected data is relevant to the originally requested information. When the CFI completes the internal analysis and review, the identified data is exported into a presentable format (such as Portable Document Format (PDF), Excel Spreadsheet, PST files, Magnet AXIOM portable case files, or a combination of these formats) which is determined by the CFI based on the readability and presentation options.

At the conclusion of a cyber investigation, a Cyber Investigation Report is sent back to the requestor (the FAA AXI investigator or the FAA legal department), and a copy is uploaded to the FAA ITS. The report contains a summary of the findings, including the FAA employee or contractor's name, email address, and location, as well as the name, email address, and phone number of the AXI investigator. Cyber investigation case files are maintained until the associated case process is completed. Once a case is completed the cyber investigation data is deleted.

eDiscovery:

The second function supported by CAVE is eDiscovery. AXI's eDiscovery team fulfills collection requests for the FAA Office of the Chief Counsel (AGC), who utilize the collected data for such legal issues as FOIA requests, litigation, Congressional inquiries, and investigations. This process is initiated once the eDiscovery Team receives a request from AGC to search FAA's internal network for electronically stored information (ESI) from requested sources, which may include government-furnished equipment (GFE) hard drives, FAA network home drives, OneDrive, shared drives, SharePoint repositories, calendar, email, Skype, Teams, and other GFE. This request can include the FAA employee or contractor's name and the reviewer's name. Upon completion of the collection, data is securely stored for analysis. An eDiscovery team member then refines the search using search terms and a date range. Lastly, data is then exported in PDF format and transferred to a shared folder for delivery to the reviewer.

Once the reviewer completes their analysis, the relevant data is exported to PDF format and transferred to a shared folder for delivery to the requestor. Once the data is delivered, the search request is complete, and the data is archived in CAVE. AGC may request a CAVE metadata report, which is used for high-volume cases. The metadata report could contain search terms and file names including the individual's name. For larger cases, the AGC may request that the CAVE administrator create a status report in Excel that lists the size of the case, the number of pages, how many reviewers, and how many documents were reviewed. The types of within PII within the report could include the FAA employee or contractor's name and the reviewer's name. The report is typically emailed to AGC and used to evaluate eDiscovery matters. eDiscovery files are maintained until the associated case process is completed. Once a case is completed eDiscovery data is deleted.

UAS Digital Storage Investigations:

The third and final function supported by CAVE is UAS investigation. AXI's UAS team receives a request to conduct a review and analysis of a UAS and its data. This data downloaded from the UAS can include the UAS owner's name and location. The UAS Team does not process a UAS investigation without a warrant from law enforcement (LE), from the FAA, or an active FAA regulatory case. Case data is collected on-site by law enforcement or FAA personnel from Extensible Firmware Interface (EFI) devices such as

common secure digital (SD) cards. Data from EFI is then delivered to UAS investigators on USB drives for manual analysis. UAS investigators also search public Internet sources for information to identify UAS operators and information that may support or refute case allegations. Once the data undergoes an internal analysis and review, relevant case data is manually transferred to CAVE for storage until the associated case process is completed. Once a case is completed, the UAS data in CAVE is deleted.

At the conclusion of a UAS investigation, a UAS Digital Investigation (UASDI) report is sent back to the requestor and a copy is uploaded to the FAA ITS. The report may contain the UAS owner's name, and location. Additionally, the report will contain the name, email address, and phone number of the AXI investigator.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

CAVE is a privacy-sensitive system because it maintains collects, uses, and disseminates PII from individuals associated with an investigation of a FAA employee/contractor for the purpose of collecting digital evidentiary data. The data collected is used to support civil, administrative, criminal, and other investigative or discoverable matters such as a FOIA case, litigation, or Congressional request. Policies, procedures, and practices for information storage, data use, access, notification, retention, and disposal are described within this PIA.

CAVE is not a system of records subject to the Privacy Act because it is not designed to be searchable by name, address, phone number, or any other PII field. Although those fields exist in the database, the system is searched by case number. As such, a System of Records Notice (SORN) is not required because the system is not retrieved by a unique identifier linked to an individual.

Access and authentication records in CAVE are covered by the Department's published SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002), which cover login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the CAVE program and/or manage the system.

Additionally, all FAA employees/contractors must review and accept the following *Terms of Use* before accessing an FAA computer:

- "You are accessing a U.S. Government information system, which includes this computer, the computer network on which it is connected, all other computers connected to this network, and all storage media connected to this computer or other computers on this network. This information system is provided for United States Government use only. Unauthorized or improper use of this information may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you consent to the following: a. You have no reasonable expectation of privacy regarding any communications or data transiting this network or stored in this information system; b. At any time, and for any lawful government purpose, the government may monitor, intercept, search and seize any communication or data transiting or stored on this information system; and c. Any communication or data transiting or stored on this information system may be disclosed or used for any lawful government purpose."

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the CAVE system.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Information collected about an individual may not be corrected since it is evidentiary data which is required in its original state for evidence to legal proceedings. Potential

legal proceedings, which may be the result of an investigation, allows individuals to correct or challenge the veracity of the data.

The data stored in CAVE originates in other FAA systems including FAA Microsoft Office 365, End User Device, Splunk, BelManage, ProofPoint Federal Production Environment, Mobile Devices/In Tune System, and ITS and arrive in CAVE via data exchanges.[3] Under the provisions of the Privacy Act, individuals may request searches of data source systems to determine if any records have been added that may pertain to them and if such records are accurate. As mentioned, the information in CAVE is received from other systems and loaded into CAVE for review. Thus individuals wanting to obtain redress and know if their PII is contained in the FAA Microsoft Office 365, and the ITS systems should follow the procedures outlined in the system's PIAs, which are located at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments/FAA.

If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

Congress authorized the FAA Administrator to develop systems and/or tools to support data collection used to support civil, administrative, criminal, and other investigative or discoverable matters such as a FOIA case, litigation, or Congressional requests. CAVE addresses the unique demands of the FAA's workforce and operates under the following authorities:

- Title 49 U.S.C., chapter 449, *Air Transportation Security*, enacted as Pub. L. 103–272 on July 5, 1994
- *Transportation Safety Act of 1974*
- *FAA Drug Enforcement Assistance Act of 1988*
- E.O., 10450, *Security Requirements for Government Employment*
- E.O. 12968, *Access to Classified Information*
- E.O. 12829, *National Industrial Security Program*

[3] Data exchanges are covered by agreements that are reviewed every three years.

CAVE collects PII for the following purposes:

Purpose: CAVE system access and program management

FAA employees and contractors

- Name, FAA Email Address, and Case Number.
- Optional Information (may be included if within the scope of the data request): Job Title, Office, Company or Organization Name, Department, Phone Numbers (Business, Home, Fax, Mobile, Pager), Business, Physical or Mailing Address, Username, IP address, Computer hostname, Alias or Nickname, English Honorific Titles, Name Suffix, such as Jr., III, or Ph.D.
- Contents of email messages and email attachments; Contact information maintained in the email user's "Contacts" function within Microsoft Outlook; Calendar entries.
- Contractor-related information: Primary FAA Contractor Officer's Full Name, Technical Officer Representative's Full Name, Contract Number, Contractor Company, Name of Prime Contractor.
- Free-form text entered into Microsoft Teams via IM; Microsoft Teams conversation history and activity feeds.
- FAA users can input information included in emails received from other members of the FAA employee and contract workforce, such as: Name, company, job title, email address, web page, address, business and home phone numbers, photographs, and notes. The data provided in the email from other members of the public, FAA and other DOT employees and contract workforce determines what information is available for input in the "Contacts" function.
- Keystrokes entered into a computer that is part of an investigation.
- Screen captures of user desktop and application windows.

Purpose: Investigation of a FAA employee/contractor (members of the public that are associated with investigation of an FAA employee/contractor)

Members of the public:

- Company or Organization Name, Case Number
- Optional Information (may be included if within the scope of the data request): name, email address, Company or Organization name, phone numbers (business, home, fax, mobile, pager), physical or mailing address, Department,

Office, Alias or Nickname, English Honorific Titles, Name Suffix, such as Jr., III, or Ph.D.

- Content of the email message and email attachments (may include other sensitive PII included at the discretion of the sender)

Purpose: Investigation of UASs

Members of the public:

- UAS Flight logs:
    - Telemetry data [altitude, air speed, Global Positioning System (GPS) coordinates, motor functions, camera details, headings]
    - UAS serial number
    - Error/update logs (GPS acquisition errors, lost signal errors, firmware errors, communication errors, network errors, time/date)
- Flight Path Pictures/Videos – pictures/videos taken by a UAS, along the flight path.
- UAS Registration Information – name, address, phone number, email address
- UAS Criminal and Regulatory Violations – pictures, video, and flight logs (related to operating without a commercial license, unregistered UAS, and other violations)

The PII in CAVE is not used for any other purposes.

CAVE uses the access and authentication information in accordance with the purposes for which it is collected under SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002). The FAA uses the access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the CAVE program and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable SORN.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

CAVE maintains the minimum amount of information to support FAA's data collection used to provide information on civil, administrative, criminal, and other investigative or discoverable matters such as a FOIA case, litigation, or Congressional requests. All data used in CAVE is transferred to applicable program once review is completed and then all data is deleted from CAVE. Access and authentication records

maintained in CAVE are handled in accordance with the following National Archives and Record Administration (NARA) approved General Retention Schedules[4] (GRS):

NARA GRS 5.6, *Security Management Records,* approved March 2022, Item 200, *Information Security Violations Records* are temporary, and should be destroyed 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use. No final records are created or maintained in CAVE.

NARA GRS 3.2, *Information Systems Security Record* approved September 2014, Item 30, *System Access Records*. Covers audit logs and system access records, which are temporary and should be destroyed when business use ceases.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The PII in CAVE is used to support data collection, which is used to support civil, administrative, criminal, and other investigative or discoverable matters such as a FOIA case, litigation, or Congressional requests and may include individuals associated with an investigation of a FAA employee/contractor.

CAVE is used as a processor of cyber and eDiscovery investigations information and for UAS data storage. All records are only data extracts from the original source systems. All final products, Adobe Portable Document Format (PDF) files or reports, which simply summarize the data, are only temporarily stored in CAVE before they are transferred to the requesting program for official processing. Once uploaded to the requestor or requestor's system, the information is deleted in CAVE, except for the UAS data, which is maintained in S3 storage until an associated case is completed.

The FAA does not use the PII for any other purpose.

Access and authentication data in cave is handled according to SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002), which covers login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of CAVE and/or manage the system.

[4] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and to promote consistent retention practices.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The FAA collects the information through manual data entry and by system-to-system data exchanges. When the PII is received through system-to-system data exchanges, the FAA protects the integrity of the information in CAVE by limiting access to authorized FAA personnel whose official duties require them to access and use the information. Audit logs are also maintained and periodically reviewed.

CAVE system administrators review data from external sources and coordinate any data quality issues with originating data source technicians as required. Some data sources are the result of individual created documents collected as evidence for an investigation. The quality of the data is limited to authorship.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the CAVE system to test security processes, procedures, and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in CAVE. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures, and posture of the system. Based on the security testing

and evaluation in accordance with the FISMA, the FAA issues CAVE an on-going authorization to operate.

CAVE implements additional safeguards to maintain the confidentiality and integrity of all PII with the system. Access control mechanisms include a role based accessed model to ensure that access to the system is the minimum required for someone necessary to perform their duties. Internal policies limit access and ensure accountability by a strict approval process for system usage. All system users are required to successfully pass annual security training that includes proper handling of PII.

All data maintained in CAVE receives the highest available level of encryption for data at rest which ensures that unauthorized data access results in indecipherable information. Additionally, data in transit, that is information being transmitted throughout network, is also protected by a high level of encryption also preventing unauthorized access to information.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121B, *"FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

DOT implements effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with CAVE are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of CAVE as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Atul Celly
System Owner
Division manager, AXM-400

Approval and Signature

Karyn Gorman
Chief Privacy
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2024.04.24 10:30:54 -04'00'