Drug Enforcement Administration

Privacy Impact Assessment
for the
Video Surveillance System

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: March 15, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Video Surveillance System (VSS) (also known as the "Pole Camera platform") allows users to view and control live video surveillance and review stored video footage that is securely collected via feed from cameras operated by the Drug Enforcement Administration (DEA). The system provides users with remote surveillance capabilities using interconnected video cameras and managed application servers. Although audio capable, DEA does not attach any audio recording hardware (microphones) to the Pole Camera platform.

Interconnected video cameras are deployed to target locations. The cameras each have some form of wired or wireless connection with a central location. The central location uses a Video Management Software (VMS) application to control the connection to the camera. The application servers are housed in secure DEA facilities and use an internal DEA infrastructure for connectivity.

Authorized DEA employees have remote access to the cameras through the VMS. Users have unique login credentials to manage and control the cameras. The VMS serves as the collection point of the transmitted video. DEA Special Agents and DEA Task Force Officers (TFOs), and any state, local, tribal and territorial (SLTT) law enforcement officers who are working with DEA in a joint investigation, may be users of the system. Subject to the oversight of the DEA Special Agent or DEA Task Force Officer assigned to the investigation, users are granted access to video streams relating only to those investigations to which users are assigned and can log into the VMS to access video and control cameras through the software. Cameras and videos are labeled and retrieved using unique identifiers assigned to the user. Users are assigned unique logins and must create a password. Once a user logs in using the unique username and password, he or she can move assigned cameras remotely in various ways. A user can also watch a live video feed and review recorded video through the VMS. Users can perform date and time searches of recorded video from assigned cameras.

Video recorded by the VSS is stored in a server on a temporary basis, until it is downloaded onto external media for placement into the case file system. The VSS does collect and maintain information in identifiable form about members of the general public, and therefore DEA is required to complete a Privacy Impact Assessment for its use, pursuant to the E-Government Act of 2002 and the Office of Management and Budget's implementing guidance (OMB M-03-22).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement

purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The VSS collects video of surveillance targets from connected cameras for law enforcement purposes in various outdoor locations accessible by the public, in compliance with the Fourth Amendment.[1] VSS is used to conduct remote surveillance on areas of known criminal activity where having enforcement officers on site could severely compromise the investigation or place the officer in imminent danger.

VSS cameras are placed in locations where the field of view covers only areas where there is no reasonable expectation of privacy. The video may also capture images of other people at, or who pass through, the target location. Case agents determine which locations will be filmed and how much of the footage of the video is case related and must be maintained. Any video footage determined to be unrelated to the case under investigation, after consultation with the federal or state prosecutor, is deleted from the VSS without a copy being made. Video that is to be maintained is transferred to external media to be handled as non-drug evidence. Video is then deleted from the VSS either after a copy has been made on external media or when the case agent determines that a copy need not be maintained. Per DEA policy, only that information which is determined to be relevant to a case, in consultation with the (state or federal) prosecutor, is retained. For security and safeguarding, the removable external media are kept in the secure DEA Evidence Vault.

VSS cameras are identified in the system by labels that are chosen by the Server Administrators. By convention, the labels used are partial street names., which are associated with the location of the connected camera. The system collects only the video that is streamed from the camera. Date and time stamps, which are taken from the server where the data originally resides, are appended to the video file to provide searching capability within the VMS. No other case related metadata or information is available within the system.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	Controlled Substances Act, 21 U.S.C. § 801, et seq., See also, 5 U.S.C. § 301, 44 U.S.C. § 3101
X	Executive Order	E.O. 12333 §§ 2.3(c), 2.6(b), as amended by E.O. 13355 and E.O. 13470 §§ 1.3(b)(5), 1.6(g), and 1.7(i)).
	Federal Regulation	

[1] To date, the four federal circuits which have considered the question, have held that video surveillance from otherwise public spaces does not constitute a "search" under the Fourth Amendment. *See United States v. Dennis*, 41 F.4th 732 (5th 2022); *United States v. Moore-Bush*, 36 F.4th 320 (1st 2022) (*en banc*); *United States v. Tuggle*, 4 F.4th 505 (7th 2021); *United States v. May-Shaw*, 955 F.3d 563 (6th 2020). The Colorado Supreme Court has held otherwise, *People v. Tafoya*, 494 P.3d 613 (Colo. 2021), while the Massachusetts Supreme Judicial Court has held that, depending on the facts and circumstances, this investigative technique may implicate the Fourth Amendment. *Commonwealth v. Mora*, 485 Mass. 360, 150 N.E.3d 297 (2020).

	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	Agents Manual sections 6634.41-6634.44

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name			
Date of birth or age			
Place of birth			
Gender	X	A, B, C, and D	Video may record the apparent gender of members of the public (USPER or not) if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
Race, ethnicity or citizenship	X	A, B, C, and D	Video may record the apparent race/ethnicity of members of the public (USPER or not) if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Religion	X	A, B, C and D	It is possible that video may incidentally record the apparent religion of members of the public (USPER or not) wearing clothing traditionally identified with certain religions (priest collars, Crucifixes, religious habits, yarmulkes, hijab, etc.,) if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B, C, and D	License plates of members of the public (USPER or not) if in the view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
Personal mailing address	X	A, B, C, and D	Partial street addresses of deployment sites are used as labels that may or may not be the same as the target address of members of the public (USPER or not); Recording/labeling of the same for DOJ or other Federal personnel may be incidentally obtained.
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Applicant information			
Education records			
Military status or other information	X	A, B, C, and D	Video may record the uniforms/ranks of members of the public (USPER or not) in the military if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Video recordings of members of the public (USPER or not) if in view of camera may potentially capture images that may be considered criminal records. Unlikely but possible to capture DOJ or other Federal personnel in those records.
Juvenile criminal records information	X	C and D	Video recordings of Juvenile members of the public (USPER or not) if in view of camera may potentially capture images that may be considered criminal records of members of the public (USPER or not);
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	The Video Surveillance system may capture static location information associated with the camera recording members of the public (USPER or not) if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Video recordings of members of the public (USPER or not) if in view of camera contain still images tantamount to photographs. Recording of the same for or other Federal personnel may be incidentally obtained.
- **Video containing biometric data**	X	A, B, C, and D	Video recordings of members of the public (USPER or not) if in view of camera may contain some images that may incidentally be analyzed for biometric data. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Scars, marks, tattoos**	X	A, B, C, and D	Video may record visible scars, marks or tattoos of members of the public if in view of camera. Recording of the same for DOJ or other Federal personnel may be incidentally obtained.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	System audits are done on DOJ and other Federal user's access
- **User passwords/codes**	X	A and B	System audits are done on DOJ or other Federal user's access
- **Date/time of access**	X	A and B	System audits are done on DOJ or other Federal user's access
- **Content of files accessed/reviewed**	X	A and B	System audits are done on DEA and other Federal user's access. Only meta data of the content in files are captured in audit trail, not the actual content.
- **Contents of files**			See note above.
Other types (please list all other types of identifying information collected and describe as completely as possible):			

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

Directly from the individual to whom the information pertains:					
In person	*X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): * Images of individuals collected and recorded from video camera					

Government sources:					
Within the Component	X	Other DOJ Components	*X	Other Federal entities	
State, local, tribal	*X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): *If VSS acquires images from other FED or SLTT partner agencies DEA will be in ultimate control of the VSS.					

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared*			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	DEA agents and TFO's can view videos of cameras assigned to them as part of an active investigation. Supervisors can view videos of cameras assigned to personnel within their authorized group. After consultation with prosecutors that footage is relevant, copies of VSS video downloaded to case files can also be shared within DEA, subject to VSS policy limitations, including a legitimate need to know.
DOJ Components	X		X	Other DOJ component personnel may be provided view-only access to cameras used in a joint investigation with DEA. After consultation with

Recipient	How information will be shared*			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
				prosecutors that footage is relevant, copies of VSS videos downloaded to case files can also be shared, subject to policy limitations.
Federal entities	X		X	Other federal personnel that are part of a joint investigation may be provided view-only access to camera feeds assigned to their active joint investigations. After consultation with prosecutors that only relevant video is downloaded to case files, such copies of VSS video may also be shared with other Federal entities, in accordance with policy and applicable routine uses,
State, local, tribal gov't entities	X		X	Any non-TFO SLTT personnel that are part of a joint investigation may be provided view-only access to VSS camera feeds assigned to their active investigation. After consultations with prosecutors that only relevant video is downloaded to the investigative file, downloaded copies of VSS video may also be shared with other SLTT entities when in accordance with policy and applicable routine uses.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		When applicable, a copy of relevant VSS video surveillance that was downloaded to removable media is provided to both prosecution and defense attorneys as part of the discovery materials and/or as evidence.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

*Any video footage determined to be unrelated or not relevant to the case under investigation, after consultation with the federal or state prosecutor, is deleted from the VSS without a copy being made.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

No data is released to the public for Open Data or statistical purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

All data collected from by the VSS is for law enforcement purposes only. Because this system is used for a law enforcement purpose and contains sensitive information related to criminal and civil investigations, it is not feasible or advisable to provide notice to individuals at the time their information is accessed by the system. Therefore, no contemporaneous notification is provided to any individual of data collected by system. Any video relevant to a prosecution will be subject to discovery.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

All data collected from by the VSS is for law enforcement purposes only. No notification is provided to any individual of data collected by system. Voluntary participation of targets of criminal investigation in the collection, use, or dissemination of images and metadata to further those investigations is impractical and would thwart law enforcement investigations. Criminal suspects have an obvious incentive not to voluntarily participate in this collection, use, or dissemination because the collection, use, and dissemination helps with the investigation and prosecution of criminal cases against them.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

All data collected from by the VSS is for law enforcement purposes only. No notification is provided to any individual of data collected by system. The procedures described in 5 U.S.C. § 552a(d) and 28 C.F.R. § 16.40 et seq. for requesting access and amendment to Privacy Act protected records apply to the extent that VSS images are covered by a system of records. Exemptions noted in 28 C.F.R. § 16.98, apply, as relevant, to targets of criminal investigation. Individuals may also request access to records under the FOIA, and exemptions apply as relevant.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls.** **Provide date of most recent Authorization to Operate (ATO):** ATO Date:9/23/20; ATO Expiration: 3/21/24 **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A
	Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: N/A
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain: N/A
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Video Surveillance is categorized as a Law Enforcement Criminal Investigation and Surveillance type system per the FIPS 199 publication. The classification has resulted in the system having a Moderate security categorization (Confidentiality, Integrity, and Availability)
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Video Surveillance adheres to the required monitoring, testing and evaluation processes enforced by both DOJ and DEA's Cybersecurity Program to ensure that information residing on the system are safeguarded and protected from misuse.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:**

	Video Surveillance adheres to the required auditing procedures detailed in the DEA IT Systems Audit Log Management Policy Instruction documentation. System logs are reviewed and analyzed at least weekly for indications of inappropriate or unusual activity and findings are reported to designated officials.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Contractors that have access to the system are required to adhere to all requirements as identified in both DEA and DOJ policies. Contractual language/requirements for contractors protect the information from unauthorized disclosure.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All component personnel adhere to the required DEA privacy-related training. There is no additional training specific to the system.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The Video Surveillance Program Management Office (PMO) works diligently with DEA's Information Security section to ensure that the key privacy and security administrative, technical or physical controls are in place to minimize privacy risks.

VSS utilizes DEA's internal network architecture to transport data, thereby inheriting a major part of its physical control mechanisms that protect data being transmitted. One aspect of this mechanism is the use of security tokens to provide two-factor authentication for authorized users. The information in the DEA system is managed and accessible only to users authorized and authenticated by the Program Managers who have need to know access. Users that require access to the system have to prove a need to know access and have to be approved by their management chain. Additionally, for the technical control in place, the Video Management Software runs on DEA's server operating system that implements various logging mechanisms to include security, access, and administrative logs.

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

Case agents are responsible for determining whether and what part of the video taken from the Video Surveillance system is relevant to the case and downloading it to removeable media for storage in non-drug evidence as part of the investigation case file within 120 days of the date the video was originally recorded. All video not downloaded within 120 days is automatically deleted by a configuration setting within the

software. VSS Video that was downloaded to removable media and placed in non-drug evidence as part of the investigation case file is retained for 10 years after the close of the file (after exhaustion of appeal rights if there is a conviction, after a prosecutorial declination or administrative closure). See, DFN 601-37 (N1-170-04-10).

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

VSS data while still stored within the VSS does not constitute Privacy Act records in a system of records as the data maintained in the system (the videos) are not retrieved by personal identifier, but rather by partial street address location of the camera and date of video. However, if the data is copied and moved into an investigative case file as non-drug evidence, it will be covered by DEA-008.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DEA-008, "Investigative Reporting and Filing System" 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May 25, 2017) (https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf)

Section 8: Privacy Risks and Mitigation

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

a. Potential Threats Related to the Collection of the Information

Privacy Risk: VSS could collect more information containing PII than needed. Overcollection could occur in two different ways: 1) collection of PII other than the target's, or, 2) collection of a target's PII that is non-relevant, incomplete, or inaccurate.

Mitigation: These risks are mitigated. VSS cameras are positioned, as best as possible, to only view the target location in an effort to minimize any the collection of unintended data. Additionally, VSS cameras are deployed to locations that have been previously determined and verified by enforcement agents to have known criminal activity, minimizing the risk of collecting non-relevant, non-target PII.

With respect to incomplete or inaccurate collection, although DEA cannot always control environmental factors or the available angles and distance for its cameras, DEA tests its installation of VSS cameras to ensure good visibility and accuracy in imaging to ensure recordings will capture all the activities occurring in the camera's field of view during its operation. Further, DEA personnel

and TFOs are trained to evaluate all available information and assess for accuracy and reliability within the context of each use of the system.

DEA personnel and TFOs also will review their recordings to determine only relevant PII is downloaded to removeable media to be kept as part of their investigation file and ensure the clip is as complete as necessary for their purposes. In fact, per DEA policy, only that information which is determined, in consultation with the (state or federal) prosecutor, to be relevant to a case is retained. Modification of data collected is not authorized.,. This review of relevant video must be conducted within 120 days of because all VSS recordings not reviewed within 120 days are deleted, helping to preserve timeliness.

Privacy Risk: PII may be collected by VSS for investigations or activities beyond the scope of DEA's Title 21 authority.

Mitigation: This risk is mitigated. The use of VSS equipment may only be authorized by a first line supervisor after an official case file is opened, which requires supervisory approval that the investigation is within the DEA's Title 21 authority or that appropriate authority has been granted pursuant to DOJ and DEA Policy to assist in a non-Title 21 related investigation. Occasionally, extraordinary circumstances or events occur that require the participation of DEA in criminal investigations, enforcement operations, or security matters that are outside the normal mission of DEA. The participation of DEA in such activities will usually be by way of assistance to another law enforcement agency or agencies having the primary jurisdiction over the subject matter. Pursuant to 21 U.S.C. § 878(a)(5), the Attorney General is empowered to delegate to DEA federal jurisdiction "to perform such other law enforcement duties [in addition to DEA's duties under Title 21] as the Attorney General may designate." This authority is exercised by the Deputy Attorney General (DAG).

In addition, under normal procedures, a case file is only opened when: (a) an arrest is made; (b) an arrest or drug acquisition (purchase or seizure) is anticipated or targeted for some future date; or (c) a systematic gathering of information targeted on an individual, or group of individuals, or a drug trafficking operation will continue for a period and in a manner typically associated with conducting an investigation. Additionally, a case file will also be opened for a scheduled regulatory investigation. Upon the opening of such a case file, a request for the use of a VSS camera is sent from the case agent to the first line supervisor for approval where DEA authority can be confirmed. prior to VSS being deployed by the Technical Operations Group (TOG)

Privacy Risk: VSS could be used to collect images of the exercise of protected First Amendment activities.

Mitigation: This risk is mitigated. VSS use is permitted only as part of an investigation approved by supervisory official who will ensure the surveillance is conducted in accordance with the DEA policy. DEA operates under guidelines that restrict the collection of records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by law or pertinent to and in scope of authorized Law Enforcement activity. DEA has a special approval process for any "enforcement procedures" that are considered "sensitive investigative activities," such as operations involving "a religious or political organization" or "the activities of the news media."

Privacy Risk: There is a risk that collected video may include innocent persons or persons who are complying with the law who are unaware their PII is being collected and have not received notice or provided consent for collection of their PII.

Mitigation: This risk is mitigated. All data collected from by the VSS is only obtained for law enforcement purposes in the course of active investigations. Therefore, the individual notice requirement is exempted by 28 C.F.R. § 16.98. Because individual notification would thwart the law enforcement investigations and prosecution of criminal cases against targets, voluntary participation cannot be accommodated in the collection, use, or dissemination of images and metadata. Prior to download to case files, the VSS platform is not a system of records under the Privacy Act. However, DEA will only download from VSS into to a case file where it is associated with those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern.

Privacy Risk: There is a risk that collected video may include innocent persons or persons who are complying with the law who are unaware their PII is being collected and have not received notice or provided consent for collection of their PII.

Mitigation: This risk is partly mitigated. DEA is publishing this PIA to provide detailed notice to the public about the data it collects via VSS. DEA also provides general notice in the applicable SORN(s). Further, all data collected from by the VSS is only obtained for law enforcement purposes in the course of active investigations. Therefore, the individual notice requirement is exempted by 28 C.F.R. § 16.98. Because notification would thwart the law enforcement investigations and prosecution of criminal cases against targets, voluntary participation cannot be accommodated in the collection, use, or dissemination of images and metadata. However, DEA will only retain VSS information associated with those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Breach by physical or technical intrusion or access by DEA-authorized personnel without a need to know could occur.

Mitigation: This risk is mitigated. VSS records are located in a building with restricted access and are kept in a locked room with controlled access, and/or are safeguarded with an approved encryption technology. DEA VSS access points are protected by physical security methods and access controls. Physical intrusions by unauthorized individuals into DEA facilities are prevented by perimeter security protections such as armed guards and video surveillance (where applicable), and physical access is controlled upon entry to all DEA buildings and facilities by PIV card readers. Within DEA facilities, the rooms containing servers with VSS data or non-drug evidence storage area for downloaded video on removable media are further protected. Access to all records are controlled and limited to approved personnel with an official need for access to perform their duties. Servers and removable media with VSS video downloads are stored:

(1) In a secure room with controlled access;
(2) in locked file cabinets; and/or
(3) in other appropriate GSA approved security containers.

Protection of information system resources is provided by management, operational, and technical security controls. The use of individual passwords or user identification codes is required to access information system resources.

Technical access controls have been implemented for access to VSS. VSS utilizes an internal DEA system to transport data thereby inheriting a major part of its physical control mechanisms that protect

data being transmitted. One aspect of this mechanism is the use of security tokens to provide two-factor authentication for authorized users. The information in the DEA system is managed and accessible only to users authorized and authenticated by PMO who have need to know access. Users that require access to the system have to prove a need to know access and have to be approved by their management chain. Additionally, for the technical control in place, the Video Management Software runs on server operating system that implements various logging mechanisms to include security, access, and administrative logs. This is to log any and all processes occurring in both the system and the management system.

DEA also employs a series of administrative controls whereby the Program Manager or Owner (PMO) approval is required prior to providing authorization to access the system. Users requesting access to the system must demonstrate a "need to know" and managerial approval prior receiving PMO approval. VSS also requires two factor authentication to gain access to the video data files on the system. The system is stored in an access-controlled area with limited access list to the area. Without access to the room and two factor authentication credentials, access cannot be attained. In the event user credentials are compromised and access is gained, an administrator is able to remove said users access from the system.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: DEA personnel may disseminate VSS PII to others outside DEA in a manner inconsistent with the Privacy Act, published SORNs or DEA policies.

Mitigation: This risk is mitigated. Prior to download of video to case files, VSS is not a system of records under the Privacy Act. Regardless, video captured within VSS while it is within the video capture technology is only shared with partnering Federal and SLTT personnel, who can demonstrate "a need to know" as officers assigned to joint investigations deploying VSS.

Further, sharing VSS video downloaded to investigative files with other third-party law enforcement entities must occur pursuant to the relevant exceptions to the Privacy Act or applicable routine uses as published in the relevant SORN, so long as its use is consistent with the use for which the recording was originally collected. See 5. U.S.C. §552a (b)(3),(7); and SORN DOJ/DEA-008, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May 25, 2017)). Such recordings may also be redacted as necessary prior to sharing to limit the scope of information shared to only that which the third party has demonstrated a need to know. The data is disseminated by exporting to external media, which is submitted as non-drug evidence and handled as such. Rules governing non-drug evidence video files are followed to mitigate any potential improper dissemination or loss of removable media containing relevant downloaded video.