# Privacy Impact Assessment

**for the**

# Office of Inspector General Video Management System

**DHS Reference No. DHS/OIG/PIA-002**

**June 21, 2021**

Homeland Security

# Abstract

The U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) is establishing the Video Management System (VMS), which is a system hosted within the Microsoft Azure cloud environment. VMS is storage solution for receiving, storing, and reviewing audio and video data in support of the investigations conducted by DHS OIG criminal investigators (Special Agents). DHS OIG conducted this Privacy Impact Assessment (PIA) because VMS data may include sensitive personally identifiable information (PII) from those individuals involved in DHS OIG investigations.

# Overview

Under the Inspector General Act of 1978,[1] as amended, DHS OIG is responsible for conducting and supervising independent and objective audits, inspections, and investigations affecting DHS programs and operations. DHS OIG promotes economy, efficiency, and effectiveness within DHS, and has a wide scope and authority to investigate fraud, abuse, and waste. In support of the OIG's mission, the agency maintains a cadre of Special Agents who are sworn federal law enforcement officers that conduct a vast array of law enforcement functions, including arrest, search, and surveillance operations. These Special Agents are responsible for conducting criminal, civil, and administrative investigations in support of the OIG's mission. The VMS is intended to support OIG investigations by providing OIG Special Agents with the capability to record and monitor via installed video surveillance systems on an as needed basis. The need to deploy video surveillance systems arises on an *ad-hoc* basis, which impairs OIG's ability to predict when and where video surveillance systems will need to be deployed. All requests to leverage video surveillance systems associated with VMS must be vetted and approved at the OIG supervisory level, and in some cases, concurrence from prosecutorial agencies may be required.

Additionally, video and audio systems are installed in OIG interview rooms for the purpose of recording and monitoring active interviews. VMS provides investigators with a tool that assists them in gathering evidence required to prove or disprove allegations of wrongdoing. VMS data will be used to gather evidence, develop leads, and aid in seeking criminal indictments or administrative sanctions against those being investigated. However, in the case of ad-hoc deployment of video surveillance, it is possible that the system will inadvertently capture audio and video of persons not subject to an investigation. As VMS consists of only audio and video data, personally identifiable information (PII) will only be in video or audio form. VMS does not permit PII to be manually entered within the system.

Audio and video stored within VMS will contain information collected only during

[1] 5 U.S.C. App. 3.

investigations. Such investigations also consist of technical audio video surveillance operations in locations that may include DHS facilities, and interviews that may disclose sensitive PII pertaining to an ongoing investigation within DHS. Audio and video data obtained through technical audio video surveillance operations is necessary to assist investigators with determining if any wrongdoing has occurred, who is involved, and when and where such violations took place. Interviews conducted in support of investigations may be recorded in order to provide a full and accurate accounting of each interview. Some of the data collected via VMS may be of a damaging or embarrassing nature; however, the information is necessary for the successful resolution of OIG investigations.

VMS will comply with the Privacy Act of 1974,[2] DHS Fair Information Practice Principles,[3] DHS 4300A,[4] and related DHS and OIG policies in order to minimize potential privacy risks. OIG will ensure that all data transmitted to VMS, as well as all data-at-rest (stored data) within it, preserves its identification and access requirements in accordance with DHS 4300A.

All data, including PII and sensitive PII, obtained during an investigation must be protected with due care and diligence by those handling the data. Only individuals with a demonstrated need to know will receive access to VMS, and such individuals will only have access to specific data as job duties require. The ability to download data from VMS will be restricted. Downloads will only be allowed if an articulable need exists, at which time the data will be provided to those with a clear need to know.

Data within VMS may be shared with other U.S. law enforcement agencies, prosecutors, and defense attorneys on an as needed basis and in accordance with applicable law. For example, investigations with overlapping investigative jurisdictions will involve investigators from two or more agencies who will be deemed to have a need to know. Prosecutors, such as Assistant United States Attorneys (AUSA) guiding the conduct of an investigation and prosecuting offenders, as well as defense attorneys representing offenders, will also be deemed to have a need to know and be provided access to the data they require.

[2] 5 U.S.C. § 552a (1974).
[3] *See* U.S. Department of Homeland Security, Privacy Office, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, Privacy Policy Guidance Memorandum Number 2008-01 (December 29, 2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[4] *See* U.S. Department of Homeland Security, DHS 4300A Sensitive System Handbook, Version 13.1, July 27, 2017, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Inspector General Act of 1978, as amended, grants Inspectors General the authority to investigate criminal activity, including the authority to seek and execute search and arrest warrants, serve subpoenas, and perform undercover operations.[5] This authority includes the lawful use of all available investigative techniques for the collection of evidence during the conduct of the investigations, which includes the use of technical surveillance and recording interviews in order to obtain a complete and accurate record of an interview.

DHS Management Directive 0810.1 assigns the OIG the responsibility to "receive and investigate complaints or information from employees, contractors and other individuals concerning the possible existence of criminal or other misconduct constituting a violation of law…."[6] This Directive also provides instructions on roles and responsibilities of DHS Organizational Elements and DHS employees pertaining to the collection of data provided to the OIG.

## 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The OIG Investigative Records System of Records Notice (SORN)[7] provides public notice, in accordance with the Privacy Act, of the privacy information collected regarding the receiving and processing of allegations that DHS employees, contractors, grantees, and other individuals or entities associated with DHS may have violated criminal law, civil law, administrative policies, and/or regulations.

The SORN supports OIG investigations and the VMS system by providing OIG with the ability to:

- Monitor complaint and investigation assignments and results; and
- Manage investigations and information provided during the course of such investigations.

The DHS/ALL-004 General Information Technology Access Account Records System

[5] 5 U.S.C App. § 6(f)(1).
[6] *See* U.S. Department of Homeland Security Management Directive System MD Number 0810.1 (June 10, 2004*), available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf..
[7] *See* DHS/OIG-002 Investigative Records System, 80 Fed. Reg. 44372 (July 27, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns. This SORN is also being updated to provide additional transparency with respect to the records OIG collects during its investigations.

(GITAARS) SORN[8] provides notice and coverage for the information collected related to audit logs and account provisioning/user access.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

VMS is going through the security Certification and Accreditation process to obtain an Authority to Operate (ATO) for a "HIGH" category system under Federal Information Processing Standards Publication (FIPS) 199 and will comply with all requirements under DHS Management Directive 4300A. The OIG Office of the Chief Information Officer is testing different VMS components and is finalizing a Technical Architectural Diagram (TAD) to record the final VMS network configuration. The OIG Office of the Chief Information Officer is also testing user access to VMS as well as finalizing access methodology. The ATO will be obtained when all accreditation processes are completed and is expected by Summer 2021.

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Retention of VMS records will be governed by N1-563-07-5,[9] Item 1, which states all investigative case files, except for those determined to be unusually significant, are temporary and are to be destroyed twenty (20) years after completion of the investigation and all subsequent actions. Destruction of the data will consist of deletion from the VMS servers. Data within VMS, related to cases determined to be unusually significant, will be permanently retained in accordance with Item 2 of N1-563-07-5.

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected as part of this system is not covered by the Paperwork Reduction Act.

[8] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[9] DHS OIG NARA retention schedule N1-563-07-5, October 11, 2007, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-07-005_sf115.pdf.

# Section 2.0 Characterization of the Information

## 2.1 Identify the information the project collects, uses, disseminates, or maintains.

The information stored within VMS is collected during OIG investigations and is necessary to resolve the matter being investigated. The information comes from interviews and technical audio video surveillance operations conducted and obtained during OIG investigations. This information is not manually entered into the system, but may be found in the audio and video records. Information may include:

- Name;
- Date of birth;
- Social Security number;
- Telephone and cell phone numbers;
- Physical and mailing addresses;
- Email address(es);
- Financial institution information;
- Business contacts;
- Vehicle identifying information; and
- Any other personal information relevant to the subject matter of an OIG investigation.

Additional information maintained within the system is used to categorize and identify the records. VMS labels audio and video files using case number, description field, and date and time stamp. The field listed as "description field" can be used to further identify the recording, such as subject name or other identifier (e.g., B Street Polecam, Camera 1).

To provision account access, the system will also maintain user PII such as name, contact information, and duty location.

## 2.2 What are the sources of the information and how is the information collected for the project?

Information sources include individuals who are the subjects of investigations, witnesses, and victims that are interviewed by OIG criminal investigators. Those interviews may be recorded. Video recordings are also collected from technical surveillance systems installed on an ad-hoc basis in various field locations.

## 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

VMS does not use information from commercial sources or publicly available data.

## 2.4 Discuss how accuracy of the data is ensured.

Any data provided and obtained during an interview or technical surveillance will be verified for accuracy as part of the investigation, with the video and audio recordings serving as an official record. OIG uses the totality of the information available to it during its investigations. Audio and video maintained in VMS will be analyzed with all other information relevant to an investigation to ensure accuracy.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that more information than necessary is collected during an investigation and maintained within VMS.

**Mitigation:** This risk is partially mitigated. OIG investigators are trained to base their investigation on the current scope of infraction and not on hypothetical future infractions. Thus, use of the received information/gathered data will be limited to that which is required to aid the investigation. While more information than is necessary may be collected during interviews with subjects of investigations, witnesses, or victims, OIG uses the totality of this information to make a determination about what is relevant to the investigation and assist with the investigation's scope. Further, maintaining all information minimizes potential claims of impropriety or incomplete information when sharing or disclosing case information related to an investigation.

Additionally, technical surveillance operations are conducted only after careful consideration of an individual's privacy.

Depending upon the type of investigation being conducted, OIG, in concert with the assigned prosecutor, determines if the surveillance operation may violate an individual's privacy rights and if the surveillance will further the investigation and support a successful prosecution.[10] OIG also conforms to *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*[11] where data collection and sharing is based on Data

[10] If the technical surveillance operation is deemed to violate the individual's rights, the investigating agent and the prosecutor have three options: 1) Obtain consent from the party affected; 2) Seek a warrant; 3) Decline to perform surveillance.

[11] *See* U.S. Department of Homeland Security, Privacy Office, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security Privacy Policy Guidance Memorandum Number 2008-01* (December 29, 2008), *available at* https://www.dhs.gov/privacy-policy-guidance.

Minimization, Use Limitation, and on a need to know basis.

# Section 3.0 Uses of the Information

## 3.1 Describe how and why the project uses the information.

As part of ongoing investigations, OIG may install surveillance cameras and associated encryption and transmission equipment in either designated OIG interview rooms or in locations associated with the investigation (e.g., on a light post, side of road, outside a point of interest). These cameras will be connected to the VMS application to record audio and video in support of ongoing investigations.

The collected information (via video/audio recordings) is used to gather evidence needed to resolve an allegation of wrong-doing by determining if a crime or other types of misconduct are in fact being committed, fully identifying each person related to a case, developing additional leads, and constructing affidavits for arrest and search warrants.

## 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

VMS does not use technology to discover a predictive pattern or anomaly. Users can manually select a recording and then select a specific date and time in order to review the data.

## 3.3 Are there other components with assigned roles and responsibilities within the system?

It is not uncommon for DHS components, and other federal agencies to conduct joint investigations with DHS OIG. For example, criminal investigators from U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), or U.S. Customs and Border Protection (CBP) can be given access to VMS if those investigators are working on an investigation with OIG. In such cases, DHS component investigators will take the necessary steps to gain temporary access to the VMS platform, such as demonstrating why they have a need to know, and then receive an assigned user role for each case the component views.

## 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There is a risk that information may be accessed without a need to know.

**Mitigation:** This risk is mitigated. Federal criminal investigators are trained on the importance of proper handling of PII and the risks associated with improper use of the interview process/surveillance. Access to VMS is permitted only to individuals with an established need to

know. Such access will be further controlled through the use of defined roles and restrictions for each case or camera as necessary.

When logging into VMS, users are presented with a banner or notification that warns users about restrictions for the use of PII, and they must acknowledge the banner in order to continue logging in. VMS is also equipped with logging features that records all user activity, and users are made aware that their VMS activities are being recorded. Information System Security Officers periodically review the logging reports to identify any unauthorized attempts or unusual trends of logging in or access to the VMS' data. These mitigation measures keep investigators aware of their responsibilities for handling PII, and the penalties for violating PII handling guidance.

# Section 4.0 Notice

## 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DHS provides notice to the public through this PIA and the OIG SORN. However, because VMS collects and maintains potentially sensitive information through audio and video capabilities related to investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is collected. For example, with regards to technical audio/video surveillance operations, no notice is provided to the subject of the surveillance. Such notice is not required by law and would prevent the resolution of a criminal investigation.

When Special Agents interact with individuals in connection with an investigation, however, those individuals are generally aware that their information will be collected. Visible signs in the reception area of DHS OIG offices, where interviews take place, notify individuals about the ongoing recordings. These signs provide notice to interviewees, before they enter the interview rooms, that -audio/video monitoring and recording is occurring. Prior to the start of an interview, interviewers may also explain to interviewees that the interview is being recorded.

## 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

There are generally no options for an individual to opt out. The information recorded and obtained is based on an ongoing investigation conducted under OIG's authorities. OIG Special Agents may determine that recording victims or witness interviews is necessary. For example, in criminal cases, victims, witnesses, and subjects always retain the right to make a statement (or not) and to end questioning at any time If someone were to request an opt out for recording, the OIG Special Agent would seek supervisory approval prior to doing so.

In administrative cases, the subject being interviewed is required to speak with OIG and

cannot opt out of recording. To do so would be the same as refusing to cooperate, which would expose the DHS employee to disciplinary action.

### 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that subjects of investigations, witnesses, or victims are not aware that they are being recorded and their information is maintained in VMS.

**Mitigation:** The risk is partially mitigated. OIG provides general notice of VMS through this PIA and the applicable OIG SORN. However, due to the nature of OIG investigations, providing specific notice could jeopardize the integrity of an investigation and present additional risk to those individuals involved. For example, if notice was provided for an investigation pertaining to contractual fraud, waste, or misuse, the individual may change, hide, or destroy evidence that may be incriminating. By not providing an individual notice pertaining to the ongoing surveillance operations it allows the OIG to track, identify, and audit behaviors that could be subject to prosecution.

Individuals who enter OIG offices for the purpose of an interview as part of an investigation are notified of the video and audio recording in place within the interview rooms. These individuals consent to being interviewed.

## Section 5.0 Data Retention by the Project

### 5.1 Explain how long and for what reason the information is retained.

PII is retained for the purpose of resolving allegations of wrongdoing and to fully identify all those related to a criminal investigation. Retention of VMS records will be governed by the National Archives and Records Administration (NARA)-approved records schedule, N1-563-07-5, Item 1, which states all investigative case files, except for those determined to be unusually significant, are temporary and are to be destroyed twenty (20) years after completion of the investigation and all subsequent actions. Destruction of the data will consist of deleting them from the VMS servers. Data within VMS related to cases determined to be unusually significant will be retained permanently, in accordance with N1-563-07-5, Item 2.

### 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a risk that information maintained in VMS for longer than necessary, especially information deemed to be unusually significant and thus maintained permanently.

**Mitigation:** This risk is mitigated. VMS data related to investigations for which all actions have been completed, including judicial proceedings, will be placed in an archived status manually

and retained for twenty (20) years according to approved NARA records retention schedule.[12] Records for investigations determined to be "significant" after a review by DHS OIG Headquarters and will be retained permanently. Significant investigations are those that involve substantive information relating to national security, allegations made against senior DHS officials, matters that attract national media or Congressional attention, or result in substantive changes in DHS policies or procedures.[13] Case files for significant investigations are also permanently retained within VMS. Only a system administrator can access these archived files, and each log in will be recorded by VMS.

# Section 6.0 Information Sharing

## 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OIG may share investigative information with other law enforcement agencies with a verified need to know, and Congress on an as needed basis, pursuant to OIG's authorities and responsibilities. Information pertaining to an investigation may be provided to the corresponding law enforcement agency or internal affairs office who may also be conducting or following up on an investigation, as well as to prosecutors and defense attorneys. Information may also be shared with the trial court as a part of the judicial process as well as the Merit Systems Protection Board (MSPB) for administrative cases pertaining to employee misconduct. Those deemed to have a need to know will be provided user access to the data they require. Such access will be further controlled through the use of defined roles and restrictions for each case or camera as necessary. Also, the ability to download data from VMS will be restricted, and downloads will only be allowed if an articulable need exists.

## 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS OIG routinely conducts criminal investigations jointly with other law enforcement agencies. These other agencies work under the same rules for conducting criminal investigations. Each agency becomes part of a joint investigation because of a shared investigative responsibility and interest. Sharing of VMS data is authorized under the DHS/OIG-002 SORN, which outlines OIG's authority to share data with:

- The Department of Justice, including Offices of the U.S. Attorneys, or other federal agency

[12] NARA N1-563-07-5, Item 1: *All Investigative Case Files except for Unusually Significant Cases,* and Item 2: *Significant Investigative Case Files*.
[13] *Id.*

conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation; and

- Appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

## 6.3 Does the project place limitations on re-dissemination?

VMS data consists of Law Enforcement Sensitive information and DHS OIG requests that external agencies not disseminate any downloaded information beyond what is necessary in order to resolve the allegations investigated or to seek an indictment and trial, if founded. Upon use of and access to VMS, users sign a disclosure agreement and Rules of Behavior, and users also receive a disclosure banner notice upon each log in outlining the restrictions for the use of PII. These documents describe the manner in which VMS information should be handled. However, a there is the risk that once information is downloaded to removable media, VMS has no further control over the information or its dissemination. OIG has attempted to remedy this by providing guidance that limits the dissemination of information on removable media to those with a need to know and keeping an audit log of downloads.

## 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

VMS user accounts include full identifying data for the account user, and will be controlled so that certain functions, such as the ability to download recordings, will be restricted to a limited number of users. VMS also logs all users' actions in the system, including attempts to download recordings and whether the download attempt was successful or not. Sharing of VMS data with other law enforcement agencies, prosecutors, and defense attorneys will be done by providing those individuals with VMS accounts to the maximum extent possible, which will be restricted to prevent the downloading of recordings. In the event it becomes necessary to download a recording to a piece of removable media, that action will be logged within VMS and memorialized via memorandum describing what was downloaded, who downloaded it, date and time it was downloaded, to whom it was provided, and date it was provided.

## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk that information from VMS will be shared inappropriately.

**Mitigation:** This risk is mitigated. If access to VMS is shared with another agency, or a

recording is downloaded to removable media, it will only be in furtherance of an investigation. Information will only be shared based on need to know to another law enforcement agency or with the prosecutor assigned to the investigation. Users will be required to sign a disclosure document for DHS OIG before any data is provided or access to VMS is granted for data related to an investigation. The ability to download a recording is only granted to a limited number of personnel.

# Section 7.0 Redress

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

Due to the nature of the information maintained in VMS, certain records may be exempted from requests for access by covered individuals, to the extent permitted by the Privacy Act and the DHS/OIG-002 SORN and associated Final Rule.[14] U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may still file a Privacy Act request to access their information, and depending on a determination made by DHS/OIG, those records may be released.

Notwithstanding, all individuals seeking access to their records may submit a Freedom of Information Act (FOIA) request at https://www.oig.dhs.gov/foia. Requests can also be made by email, telephone, or mail:

OIG Office of Counsel
245 Murray Lane SW Mail Stop - 0305
Washington, D.C. 20528-0305
Phone: 202-981-6100
Fax: 202-245-5217
FOIA.OIG@OIG.DHS.GOV
DHS OIG FOIA Request Form

OIG only maintains ownership of its own data. Therefore, OIG will refer FOIA and Privacy Act requestors seeking non-OIG data to the appropriate the DHS component. All requests must conform to the Privacy Act regulations set forth in federal regulations[15] and are evaluated to ensure that the release of information is lawful, will not impede an investigation, and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

[14] *See* Final Rule for Privacy Act Exemptions, 75 Fed. Reg. 67909 (November 4, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[15] 6 CFR Part 5.

### 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures for correcting inaccurate or erroneous information are similar to the redress procedures in Section 7.1 above. Individuals may not be able to correct the record for information within VMS because it may be part of a confidential investigation and releasing an individual's records may impede the investigation. However, covered individuals may submit a Privacy Act Amendment request as outlined above.

### 7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA and the DHS/OIG-002 SORN provides notice to individuals regarding how to access and correct their information. Requests to amend or correct information about themselves will be handled under the Privacy Act of 1974, 5 U.S.C. § 552a(d). In addition, during an interview, the interviewing agent will inform the interviewee how he/she can contact the interviewing agent in order to provide any additional information or update/correct anything related to the interview/case. This information will be provided verbally, and interviewing agents routinely provide a business card as well.

### 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** There is a risk that individuals may not know the redress mechanism available to them for their data maintained in VMS.

**Mitigation:** This risk is partially mitigated. This PIA and the DHS/OIG-002 SORN provide information on how to request access and amendment to information maintained within VMS. Additionally, OIG informs individuals who are witnesses or victims about how to amend/correct information provided during an interview. However, individuals whose information is captured by technical audio/video surveillance operations are not provided notice of any redress procedures.

Individuals under investigation are not generally informed until the end of the investigation, and thus, the individual may not know how to apply for redress. Nevertheless, whether or not an individual is notified due to an investigation's conclusion, individuals have the ability to inquire about the information the federal government maintains on them. They have the ability to submit a FOIA or Privacy Act request, as applicable, to DHS at any time. If the individual's request to obtain records is denied in full or in part, the individual has the right to appeal their denial to the FOIA/Privacy Act Appeals Unit.[16] Individuals also have the opportunity to seek dispute resolution services through the FOIA Public Liaison, whose contact information

[16] Information on submitting an appeal is set forth in the DHS regulations at 6 C.F.R. § 5.8.

can be located on the DHS OIG website.[17]

# Section 8.0 Auditing and Accountability

## 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

VMS requires the use of two-factor authentication for access and users are configured based on Role Based Access Control (RBAC). Users may only access VMS through the OIG network. Audit logs are configured to track any user login attempts and all activities while logged into VMS, including what cases or recordings within a case a user accessed. VMS will also log any modification made to the system, which user made the modification, and date and time of the modification. The OIG Office of Chief Information Officer, Information System Security Officer for VMS will review the logs on a monthly basis. Additionally, the OIG security team will perform the following audit techniques within VMS:

- Independent Verification and Validation (IV&V);
- Risk Assessments;
- Vulnerability Scanning; and
- Third-party audits.

The OIG is also subject to inspection by the Committee on Inspector General Integrity and Efficiency (CIGIE).[18] These inspections may review the OIG's use of video surveillance and VMS in order to determine if the system is being used in accordance with its stated purpose.

[17] *See* www.oig.dhs.gov/foia.request.
[18] CIGIE is an independent entity established within the Executive Branch to address integrity, economy, and effectiveness issues that transcend individual government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the Offices of Inspectors General. *See* https://www.ignet.gov/.

### 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS OIG users are required to participate in mandatory annual trainings entitled *Privacy at DHS: Protecting Personal Information* and *HQ IT Security Awareness and Rules of Behavior*. The DHS OIG Training and Development Catalog also has a list of reoccurring mandatory trainings. Personnel are also assigned OIG user security awareness training as required within VMS. Furthermore, federal criminal investigators are trained on the risks associated with improper use of the interview process/surveillance.

### 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to investigative information is determined by case assignment. A DHS OIG office supervisor, such as the Special Agent in Charge or Assistant Special Agent in Charge, will assign investigators to an investigation and notify the case agent of the assignments. When a case involves a multi-agency investigation(s), the supervisor(s) from external agencies will provide the DHS OIG office supervisor with a representative from the (external) agency. Access to VMS is controlled, and therefore those designated representatives will receive a login once their need to know status is established. Such access will be further controlled through the use of defined roles and restrictions for each case or camera as necessary. Investigators are considered to have a need to know for case specific access, while AUSAs and defense attorneys are provided a "read-only" user access.

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All project reviews, approved information sharing, Interconnection Systems Agreements (ISA), Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), and other new data information uses for VMS must comply with DHS Sensitive Systems Handbook and Policy Directive 4300A. All appropriate documentation and requirements must be approved by all authorizing officials of each system such as:

- System Owner (SO);
- Chief System Security Officer (CISO);
- Information System Security Manager (ISSM);
- Information System Security Officer (ISSO); and

- Program Manager (PM).

## Contact Official

Edgardo Rosado
Office of Investigations
Office of Inspector General
U.S. Department of Homeland Security
(954) 547-1354

## Responsible Official

Roy Jones
Division Chief-Information Law and Disclosure
Office of Inspector General
U.S. Department of Homeland Security

## Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717