Privacy Impact Assessment

Office of Safety, Security and Protection

Policy, E-Government and Fair Information Practices

- Version: 1.2
- Date: 12/30/2024
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

Privacy Impact Assessment for the

Video Surveillance System

CSAM ID 2571

12/30/2024

Contact Point

Samuel Willis
Office of Safety, Security and Protection
202-378-5830

Reviewing Official

Michele Washington
Privacy Officer
Departmental Administration Information Technology Office
United States Department of Agriculture
202-205-3369

Abstract

The U.S. Department of Agriculture's (USDA)Video Surveillance System (VSS) is built on a COTS Application Avigilon Control Center. The system is designed to capture, view and replay video footage within the National Capitol Region (NCR). The PIA is being conducted because the Video Surveillance System is capturing and storing video footage of USDA employees, contractors and visitors as they enter and traverse the USDA NCR buildings.

Overview

The mission of USDA Office of Safety, Security and Protection (OSSP) Video Surveillance System (VSS) is to keep property safe and secure for federal employees; to provide a cost-effective method to monitor a location, provide archived video coverage for investigations; and to deter against future crime or attack. OSSP is responsible for the protection of federal facilities, staff, and visitors, which may be the target of acts of terrorism or other crimes such as robbery, burglary or vandalism. Crimes in progress may be detected and possibly prevented since the video feeds can be monitored in real-time. Also, a clearly visible camera alerts the public that they are being monitored, which may deter criminal activity.

VSS supports OSSP's compliance efforts for the video surveillance components of the. VSS is owned and operated by USDA Data Administration (DA)/OSSP/Facility Projection Division (FPD).

VSS provides a secure and cost-effective means for OSSP to deploy video surveillance for the NCR; supports the mitigation of identified threats and vulnerabilities; and assists in assuring unauthorized individuals do not gain access to critical USDA assets. Additionally, VSS will assist OSSP with its role in securing and protecting the USDA NCR by being a force multiplier for on-site security services.

VSS is built on a Commercial off the Shelf (COTS) product, Avigilon Access Control Center (ACC) and can utilize any analog or IP based camera for collecting video footage. VSS allows for the recording, live viewing, archiving and playback of recorded video for electronic surveillance applications. VSS performs viewing, playback, and video storage functions simultaneously. VSS is an open standard, network-based software platform that is user friendly for both officers and administrators alike. VSS is designated an industrial control system, Supervisory Control and Data Acquisition (ICS/SCADA) system (NIST SP 800-82).

Privacy protections for VSS systems include limiting access to the video feed to only authorized users and establishing clear auditing systems so every use of the VSS system is logged and reviewable and restricting storage. Also, USDA OSSP VSS users agree to a "Rules of Behavior" which subjects employees to administrative and potentially criminal penalties if any misuse occurs.

VSS collects and stores streams of video images by location, date, and time. VSS captures images on video. Surveillance cameras are meant to keep people and property secure.

Cameras are there not to invade a person's privacy, but to protect the public by deterring criminal activity and by providing material evidence when a crime has been caught on video.

Section 1.0 Characterization of the Information

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

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

The only data collected, disseminated, and maintained by the system is video footage of areas throughout the USDA NCR.

USDA places the VSS cameras around the perimeter and inside of USDA facilities and buildings, including parking lots, entrance and exits, and secured areas. The VSS cameras may capture facial images of employees and visitors to USDA buildings and images of license plates that are parked or drivingthrough the parking lot.

Additionally, some VSS collect metadata. Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. Regarding a VSS, some examples are camera name, location, time, and date. The data is used to manage the VSS feeds and footage files.

USDA uses the VSS's video feeds captured through cameras to aid in crime prevention and criminal investigations, enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation or terrorism prevention.

VSS recordings may provide investigators with leads when investigating crimes occurring at protected federal facilities. For example, VSS records may assist investigators in identifying persons who were in the area when a crime occurred, or identify suspects or vehicles fleeing the area. These videos may also become evidence in a subsequent criminal prosecution.

Camera images can provide USDA personnel with real-time information on suspicious activities that may be related to terrorist activity, such as terrorist surveillance or actions in preparation for a terrorist attack. In addition, the camera recordings can be used for investigative and prosecutorial purposes in the event of an

attack. USDA uses VSS's images to identify individuals and may try to identify individuals through other data elements like a license plate number captured by a VSS camera feed.

Cameras are not placed in places with a reasonable expectation of privacy such as inside a bathroom or changing room.

1.2 What are the sources of the information in the system?

The sources of the video footage are IP Based and Analog Based Video Cameras throughout the USDA NCR.

VSS records video from a variety of ranges and with differing zooming capabilities. The cameras may record passersby on public streets and USDA personnel accessing a secured area. The VSS cameras collect video images through real-time monitoring with streaming and storage onto a storage device.

Zooming capability allows for the recording of textual information such as license plate numbers or text written on a person's belongings. Cameras contain low-light technology to support detection of unauthorized or suspicious activities at night. Most cameras are fixed but others use pan/tilt/zoomcapability with manual tracking, which allows the individual monitoring with the VSS feed to adjust the camera in real time to gain the best image of any suspicious or illegal activity of interest that is occurring. Tracking, which can be manual or occur when the cameras automatically track people or other moving objects in the field of view is used so security personnel may follow the activity of a single individual within viewing areas that contain a large number of people.

The video footage includes images of people, information found on drivers licenses such as full names, addresses, date of birth, as well as license plate numbers.

1.3 Why is the information being collected, used, disseminated, or maintained?

The surveillance footage is being collected to keep people and property secure. The videos are used to protect the public by deterring criminal activity and by providing material evidence when a crime has been caught on video.

1.4 How is the information collected?

The information is collected by the analog and IP based cameras in the NCR.

1.5 How will the information be checked for accuracy?

The information will not be checked for accuracy. The video footage is stored just as it was collected.

VSS cameras collect real-time video of the activities occurring within their viewing space in or near USDA buildings. The videos are altered through a compression algorithm in order to be stored in an array of hard drives but otherwise are not modified or changed to alter the recorded activities. VSS cameras only record what is occurring in real time; there is no editing feature or ability to change the image.

Only authorized personnel have access to the stored video data, and all USDA personnel must agree to a general "Rules of Behavior" before logging into any USDA system. The "Rules of Behavior" listthe specific uses for the system and a notice that use of the system is audited through logs. The misuse of any system will subject employees to administrative and potentially criminal penalties. Additionally, VSS access is restricted to only authorized users.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

7 CFR section 2.24(a)(8)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: The cameras will collect more information than is necessary to accomplish the purpose by the VSS.

Mitigation: This is mitigated by the placement of cameras in public places as opposed to bathrooms or other areas where individuals have a reasonable expectation of privacy. The purpose of VSS is to protect the buildings, grounds, and property owned, occupied or secured by the federal government, and the persons on the property. VSS is only used to render property safe and secure as well as to deter future crimes or attacks.

Privacy Risk: Video that is not relevant and necessary to accomplishing the mission will be collected and not recorded over.

Mitigation: USDA only uses the video feeds to detect and respond to potentially unlawful activities in real time or to support law enforcement investigations and prosecutions to the extent that they contain information relevant to a criminal (or

potential criminal) activity. All other video feed is automatically overwritten once the storage capacity has reached its limit.

This is also mitigated by the "Rules of Behavior" users must sign and by administrative and potentially criminal penalties.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The information collected by the VSS will be used to monitor activity throughout the USDA NCR in real time, it will be used to review events that have taken place in a post investigative nature and may be exported to be used later for criminal or disciplinary actions.

2.2 What types of tools are used to analyze data and what type of data may be produced?

All tools used are COTS products packaged with the Avigilon Control Center software. VSS is an industrial control system with cameras that captures video pictures.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: VSS may be used for improper surveillance or record more than is necessary.

Mitigation: The purpose behind USDA use of a VSS is to detect and deter criminal activity, and to provide investigatory leads only.

Additionally, VSS access is restricted to only those who monitor the video feeds. The system tracks the users and will be periodically reviewed for misuse and discriminatory practices.

"Rules of Behavior" must be agreed to before any use of the system. The misuse of any system will subject employees to administrative and potentially criminal penalties.

Privacy Risk: Unauthorized access to a VSS video feed may occur.

Mitigation: The risk is mitigated by the fact that the video feed is encrypted during transmission and only videos of stored data are available.

Privacy Risk: Use of VSS cameras may restrict freedom of speech or association.

Mitigation: The system does not in any way restrict freedom of speech or association. The images are primarily used to detect and deter criminal activity. The images are not used to restrict or investigate lawful rallies and associations. The occurrence of First Amendment-protected activity, such as a protest or rally outside a federal facility, is treated by USDA like any other activity that may be captured by a USDA camera. Unless there is evidence of criminal activity that must be investigated or prosecuted, USDA will not maintain those images for longer than the storage capacity of the VSS. USDA shares images only for legitimate law enforcement purposes or in response to FOIA requests.

Section 3.0 Retention

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

3.1 How long is information retained?

The intent is a 6-month retention period for all video footage, however, depending on storage, camera counts and other factors, video may be retained for longer, but will be over-written on a first in first out basis. Data is stored for a maximum of six months and then is automatically deleted.

Records which are retrieved pursuant to suspected criminal activity will be retained until any investigative or enforcement action is completed. To retain the footage after the retention period, a supervisor must approve the request and confirm the recordings are relevant to actual or suspected criminal activity.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

USDA stores recorded video for six months after which the video is automatically deleted in accordance with National Archives and Records Administration (NARA)

General Records Schedule (GRS) 5.6, item 090 (DAA-GRS-2017-0006-0012 (Facility security management operations records).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a privacy risk that storing video for six months is too long.

Mitigation: The retention period is appropriately limited to only retain images for a short length of time, while still allowing USDA to identify potentially relevant video when a crime has occurred but is not immediately reported.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Video footage will only be shared with internal organizations in response to formal requests, such as criminal investigations and disciplinary actions.

4.2 How is the information transmitted or disclosed?

The information can be transmitted via media, such as CD or DVD and/or may be transmitted as exported video clips in a variety of video formats. In any case the video footage will be encrypted, and password protected when transmitted.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Internal information sharing will be minimal, any risks are mitigated by using sign-in protection.

Risk when sharing within USDA is considered low-moderate. When data sharing within the network, encryption protocols ensure PII is not inadvertently shared in an unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with a need-to-know using internal, granular governance process. Dissemination of information is governed by internal policy. Internal information sharing is limited to the VM server boundaries within the information systems. The data is encrypted into unique data strings to further mitigate any risks to PII.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Video footage will only be shared with external organizations in response to formal requests, such as criminal investigations and disciplinary actions

Information from the VSS cameras will be used by federal agencies and local law enforcement to detect and respond to potentially unlawful activities in the areas surrounding federal facilities. The information may also be used to support law enforcement investigations and prosecutions to the extent it contains information relevant to a criminal or potentially criminal activity. For example, if a suspicious package is placed outside a federal building, the system allows federal officials to take appropriate responsive action. Additionally, if the package is determined to be an explosive device, the recordings could be used to further investigate this criminal activity, assist in identifying the perpetrators, and/or provide evidence that may be used in court.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, the sharing of PII outside USDA is compatible with the original collection of the data for protecting USDA resources.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information can be transmitted via media, such as CD or DVD and/or may be transmitted as exported video clips in a variety of video formats. In any case the video footage will be encrypted, and password protected when transmitted.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Risk: Authorized disclosure due to the method in which the data is shared to external organizations.

Mitigation: Video footage will only be shared with external organizations in response to formal requests, such as criminal investigations and disciplinary actions

Information from the VSS cameras will be used by federal agencies and local law enforcement to detect and respond to potentially unlawful activities in the areas surrounding federal facilities. The information may also be used to support law enforcement investigations and prosecutions to the extent it contains information relevant to a criminal or potentially criminal activity.

The information can be transmitted via media, such as CD or DVD and/or may be transmitted as exported video clips in a variety of video formats will be encrypted, and password protected when transmitted.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

No.

6.2 Was notice provided to the individual prior to collection of information?

Yes, signs are visibly displayed to inform of the use of active cameras throughout the facility. VSS provide notice of the surveillance camera. Signs are posted in public areas, in written format. An example of the type of wording provided in such notice signs is:

"WARNING: Premises Protected by 24 hour video surveillance"

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Individuals who enter, or are near federal property, do not have a reasonable expectation of privacy and therefore no consent is required. However, as a matter of policy, signs are posted to provide notice of surveillance activities via VSS's cameras.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Members of the public may not see the notice sign or may not be aware of why cameras are necessary.

Mitigation: The risk is mitigated by the publication of this PIA. This PIA makes clear that federal properties are under surveillance by cameras and why the cameras are necessary. Additionally, it has been a requirement since the 1995 Presidential Policy Memorandum for Executive Departments and Agencies titled *Upgrading Security at Federal Facilities* for federal facilities (where feasible) to install cameras. Federal buildings must be protected, and cameras are a cost efficient and useful tool to prevent crime and terrorism. The use of cameras is a common practice throughout the United States in the private, commercial, and federal arenas and is a standard security practice.

Section 7.0 Access, Redress and Correction

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

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

Individuals may access their information by submitting aFOIA/Privacy Act request to the FOIA Officer, 1400 Independence Avenue SW, Washington, DC 20250 or by email at USDAFOIA@usda.gov. VSS does not record or retrieve information by personal identifiers so it will be difficult for an individual to find and view a particular video. Additionally, videos are only stored for a maximum of six months. The video is then recorded over, which limits the amount of time an individual has access to the video. Accordingly, an individual wishing to access their information should provide a detailed description, such as the address or physical location of the camera, the date and approximate time the video or image was taken, or other identifying information that will assist USDA in locating the requested record. For more information on specific procedures for submitting a FOIA request, see https://www.dm.usda.gov/foia/ .

7.2 What are the procedures for correcting inaccurate or erroneous information?

Video image cannot be corrected given it captures the events in real time, but an individual may complete a FOIA request to view the image.

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

Individuals are not notified of procedures for correcting their information as the data is collected directly from the camera.

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

The individual has the ability to contact USDA, Office of Safety, Security and Protection,1400 Independence Avenue SW, Washington, DC 20250. Also, available is the ability to contact the Facility Protection Division Help desk at

FPDServiceHelp@usda.gov or call (202-720-6270) to address any information correction issues.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: The period of time for redress for an individual is very short. In most cases, video is not retained longer than six months.

Mitigation: Given the nature of VSS, a robust program to permit access, review, and correction of the video cannot be provided. This lack of direct access and formal redress mechanism represent a risk to individual privacy; however, it is necessary given the utility of VSS and the retention rates. While some individuals will not have a formal mechanism for access or redress, USDA has internal mechanisms to correct inaccuracies and protect against abuse through the auditing system and the "Rules of Behavior" for users.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Only authorized users are allowed to view the video feeds of VSS. The log-in and use of the system is traceable to a particular user and periodically audited for misuse and discriminatory practices.

The system is audited when an employee with access leaves the organization or when called for by a supervisor. The audit is performed by someone within the organization but separate from the operational team.

VSS users will be required to fill out and sign a User Account Request (UAR) which includes a Rules of Behavior that will be approved by the System Owner or their delegate before a user is granted access to the system. This UAR will outline the intended use of the system and any actions that will be taken against the user should they misuse the system or information.

8.2 Will Department contractors have access to the system?

Yes. Access to VSS will be granted for both USDA employees and select non-employees with appropriate background checks and security clearances in place.

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

Training is provided to all USDA employees and contractors on handling of PII and correct uses of relevant systems. Training includes privacy, technical aspects of the system, and disciplinary procedures for violations.

8.4 Has Assessment and Authorization been completed for the system or systems supporting the program?

Yes; authorization date 12/23/24

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system is audited when an employee with access leaves the organization or when called for by a supervisor. The audit is performed by someone within the organization but separate from the operational team. Also, quarterly security audits are conducted on the system and users.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Unauthorized access or a data breach.

Mitigation: Only authorized users are allowed to view the video feeds of VSS. The log-in and use of the system is traceable to a particular user and periodically audited for misuse and discriminatory practices. VSS is also physically protected against unauthorized access.

Finally, “Rules of Behavior” must be agreed to and signed before any use of the system. The misuse of any system will subject employees to administrative and potentially criminal penalties.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

VSS is operating under a Moderate security categorization per FIPS 199. VSS collects video footage from around the USDA NCR. It will rely on the USDA network to route IP Based video footage to Network Video Recorders and Video Surveillance Workstations.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

No, VSS does not employ technology which may raise privacy concerns. All privacy concerns are mitigated by three factors, which are all required by USDA guidelines per NIST recommendations. The first factor is that individuals must meet the requirements of the USDA two factor authentication process. This includes having a LincPass. Secondly, all individuals who access VSS data must request access via VSS designated authority. Access is granted following approval by the change control process or directly by the Chief, OSSP FPD. Thirdly, following the approval of credentials, all individuals who obtain access to VSS must acknowledge and agree to the terms of the Rules of Behavior.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

No 3rd party websites or applications will be used.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

No 3rd party websites or applications will be used.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

No 3rd party websites or applications will be used.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

No 3rd party websites or applications will be used.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

No 3rd party websites or applications will be used.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

No 3rd party websites or applications will be used.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

No 3rd party websites or applications will be used.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No 3rd party websites or applications will be used.

10.10 Does the system use web measurement and customization technology?

No 3rd party websites or applications will be used.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

No 3rd party websites or applications will be used.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

No 3rd party websites or applications will be used.

Agency Approving Officials

_____

Samuel Willis
System Owner
Office of Safety, Security and Protection
United States Department of Agriculture

_____

Lisa McFerson
Information System Security Manager
Departmental Administration Information Technology Office
United States Department of Agriculture

_____

Michele Washington
Privacy Officer
Departmental Administration Information Technology Office
United States Department of Agriculture

_____

Sullie Coleman
DAITO CISO
United States Department of Agriculture

QUANISHA JONES Digitally signed by QUANISHA JONES
Date: 2024.12.30 02:07:42 -05'00'

_____

Office of the Chief Privacy Officer
United States Department of Agriculture