Privacy Impact Assessment for the VA IT System called:

Knightscope Autonomous Security Robot (ASR) -E

Veterans Affairs Corporate Office (VACO)

Veterans Affairs Police/Physical Security

eMASS ID #2109

Date PIA submitted for review:

1/18/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	OITPrivacy@va.gov Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Scott Miller	*Scott.miller@va.gov*	*717-413-1940*
Information System Owner	*Scottie Ross*	*Scottie.ross@va.gov*	*(478) 595-1349*

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Knightscope Autonomous Security Robot (ASR) project is to enhance the VISN 17, South Texas Health Care System Veterans Affairs Police ability to monitor activity within the patrolled areas, enforce campus parking requirements, identify and respond to anomalies and events in a timely manner, increase the visibility of security in defined areas to deter criminal, noncompliant and other undesirable behavior, and to demonstrate the functionality of the ADM (Autonomous Data Machine/K5) for consideration in other applications for the STVHCS business interests. The ADM/K5 does not have the program for biometrics/facial recognition and can't determine a human form yet can recognize an anomaly such as a human, animal or other entity that may be on its patrol path and alert VA Police to respond. The Amazon Web Services Government Cloud (AWS) (non-VA) is where patrol activities are stored for 30 days then removed permanently.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Knightscope Autonomous Security Robot (ASR); Veterans Affairs Police/Physical Security

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

Knightscope Autonomous Security Robot (ASR) project is to enhance the VISN 17, South Texas Health Care System Veterans Affairs Police ability to monitor activity within the patrolled areas, enforce campus parking requirements, identify and respond to anomalies and events in a timely manner, increase the visibility of security in defined areas to deter criminal, noncompliant and other undesirable behavior, and to demonstrate the functionality of the ADM (Autonomous Data Machine/K5) for consideration in other applications for the STVHCS business interests. The ADM/K5 does not have the program for biometrics/facial recognition and can't determine a human form yet can recognize an anomaly such as a human, animal or other entity that may be on its patrol path and alert VA Police to respond. The Amazon Web Services Government Cloud (AWS)(non-VA) is where patrol activities are stored for 30 days then removed permanently.

C. Who is the owner or control of the IT system or project?

Veterans Affairs Police/Physical Security - controlled

Knightscope - vendor owned

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

There are two groups on individuals who will have data stored.
The Users with access to the User interface will have their emails stored in the system, as well as their phone number if they provide it. That will be approximately 86 Police Staff.

The public group will consist of individuals, whose likenesses will be captured on video as well as license plates captured on video, while the K5 robot is patrolling VA controlled property.
This will equate to approximately 75 individuals and/or vehicles per hours.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The Knightscope Robot will be used as a force additive for patrolling the outside of VA Facilities that have the VA Police presence. The Robot will be responsible for traversing a defined set of GPS Way Points that are programmed into the Robot along with its power docking station. The main purpose of the system is to act as a type of VA Police presence and added manpower to allow manpower to be assigned other places as needed. The information collected is going to be either a video file and/or an audio file when the Robot is activated to collect such information. The information collected on VA Employees and Contractors is collected so accounts and login ability can be done for them so they can access the KnightScope IaaS platform.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

Currently the VA does not externally share information from the Knightscope SaaS and does not plan on doing so. The VA Police does share the Knightscope information internally between VA Police Activities following Policy, Procedures and SOPs.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

The Current solicitation is specific to San Antonio, TX. While it is foreseen that this may be deployed elsewhere, it is not currently deployed, nor is it currently being solicited by other facilities.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

103VA07B/73 FR 74580 Police and Security Records-VA This system contains records relating to veterans, VA employees and other individuals who have been a complainant or witness to a crime or accident or had a VA identification card prepared for them.

The SORN is defined by VHA RCS 10-1 Item # 5252.10 Chapter 5, 5252 Police Records Items 5252.9, 5252.10, and 5252.28

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

No

K. Will the completion of this PIA could potentially result in technology changes?

No

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☒ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements
Video Images
Work Active Director Login Information
Work Phone Number
Photographs

NOTES:
Part of the information is collected due to the employment of the VA Employee and VA Contractors information which includes First and Last Name, Active Directory Login Information and Work Phone Number are collected for creating login accounts for the Knightscope SaaS web portal.
Vehicle License Plates could be an incidental piece of data collected in a video or audio file.
Facial recognition is NOT turned on for this system and is NOT intended to be used and is NOT available in the version of Knightscope K5 v5.2 that the VA has contracted.

PII Mapping of Components (Servers/Database)

Knightscope Autonomous Security Robot consists of 1 Key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Knightscope Autonomous Security Robot and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
KnightScope VA System	Yes	Yes	Name, Work Phone number, Video,	User credentials, Public Safety and Law	TLS 1.2 WPA2(E) and AES 256

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

			license plates, photographs, work active directory login information, or voice recordings	Enforcement Investigations	

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The K5 robot is an autonomous robot on continuous patrol. It collects data through sensors and cameras from the categories below. It does not allow external input of data only the continuous collecting of data.
Veterans or Dependents, VA Employees, VA Contractors, Members of the Public/Individuals, Volunteers and Clinical Trainees

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

VA Active Directory Login Information is collected to create VA Employee or VA Contractor accounts in the Knightscope KSOC portal for interaction with the collected video and audio files along with the Knightscope K5 robot.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Yes. The system creates reports, for example: Login Records, Error Reports, Plates detection Report, Parking Meter Report, Approved Plates Report, Denied Plates Report, Alerts Report, LTE Usage Report, Machine Stats Reports.

Data collected and reports generated will be used for VA Police reporting. No additional data will be input to the system, or added to the native Knightscope reports while housed in the Knightscope environment.

The system

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The information is collected directly from the authorized members of the police department in the creation of the user credentials.
The police department is also authorized to input a license plate number into the KSOC watch list. Information from the KSOC is created by the K5 and sent to the KSOC to live stream video or alert the police department of an anomaly within specified parameters.
The K5 Robot takes the video and audio clip by recording it and placing it in the VA Designated Storage container for future work.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

The information is collected automatically and stored in the Knightscope environment until utilized. No external forms are needed.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

All available security measures utilized in SSOI to ensure that users are verified in the Active Directory.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, the system does not check for accuracy by accessing a commercial aggregator.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

103VA07B/73 FR 74580 Police and Security Records-VA This system contains records relating to veterans, VA employees and other individuals who have been a complainant or witness to a crime or accident or had a VA identification card prepared for them.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Potentially the wrong personal could see the privacy data created by the system.

Mitigation: The proper levels of permissions are given to the VA Police personnel and the system is configured to match the FedRAMP security controls which are encrypted system or SaaS connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions. The collected information will only be used in an approved VA Official capacity.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Active Directory Login Information (Email)	Provides access to the system for each user, it identifies each user	Not used

Name (Frist and Last) – VA Employee and Contractor	Used in Account Creation for VA Employees/Contractors and used to greet the user accessing the KSOC	Not Used
Work Phone Number	Used in Account Creation for the VA Employees/Contractors and if provided by the user, it will be used to send them alerts about what the system has detected	Not Used
Licenses Plate Number	Only used to match automobiles to a list of Be-on-the-lookout plates that the VA will enter the system	Not Used
Video	Used to collect information from either someone at the VA Police location and the incident occurring	Not Used
Audio	Used to collect information from either someone at the VA Police location and the incident occurring	Not Used
Photographs	Occurs after the VA Police have reviewed the video and audio recordings. A still photo can be collected and are uploaded to the Knightscope IaaS.	Not Used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

User's information is only used for access purposes only, no reports are generated based on that which would be used by either Knightscope or the VA. There is no derived data from it either.
The reports that will be generated will include information specific to the robot and will not generate reports based on the data collected by Video Surveillance.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the

individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

No, there is no individual records in the Knightscope SaaS system, but the data maybe shared internally to the VA Police for public safety and emergency situations that could lead to VA Police reports and criminal investigations.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

VA baseline security controls are in place for VA systems (laptops) that are FIPS 140-2 and 140-3 compliant. The Vendor uses the same FIPS 140-2 and 3 compliant security controls which are encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The system is not intentionally collecting SSN information.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1.The information with each application is categorized in accordance with FIPS 199 and NISTSP 800-60. As part of the categorization any PII is identified.

2.The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

3.The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The proper levels of permissions are given to the VA Police personnel and the system is configured to match the FedRAMP security controls. The collected information will only be used in an approved VA Official capacity.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, documented in FedRAMP Control SOPs

2.4c Does access require manager approval?

Yes, per VA Policy.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes, per VA and FedRAMP Policy.

2.4e Who is responsible for assuring safeguards for the PII?

System Owner/VA Police.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

First/last name, Active Directory Login Information, license plate numbers, work phone number, video, audio, and photos.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Video information is only retained for 30 days as set forth in the deployment requirement of the VA Police Department. It is then written over with new video and is akin to using a CCTV networked video recorder. Specific anomaly notifications (i.e., a person observed in the area after hours or a license plate the police department has identified as a threat) are generated based on specific requirements of the police department are archived and retained for the life of the technology use by the police department.

VHA RCS 10-1 Item # 5252.10 Chapter 5, 5252 Police Records Items 5252.9, 5252.10, and 5252.28

Records of Routine Security Operations – VHA RCS 10-1 Item# 5252.9

Records about detecting potential security risks, threats, or prohibited items carried onto Federal property or impacting assets, including records documenting access control, screening, patrol and response, and control center operations. Includes:

•surveillance records

•recordings of protective mobile radio transmissions

•video surveillance recordings

•closed circuit television (CCTV) records

NOTE: Records of accidents and incidents are covered under item 100 and records of visitor processing are covered under items 110 and 111.

EXCLUSION: Law enforcement officer-related records, which are covered by agency-specific schedules. Temporary. Destroy when 30 days old, but longer retention is authorized if required for business use. GRS 5.6, item 090 DAA-GRS-2017-0006-0012

Incident transferred to a different record series

Accident / Incident Records – 3 years after final investigations

VHA RCS 10-1 Item# 5252.10

Maintained as an active file based on case being open or closed

Once case is closed – 3-year countdown begins at the end of that calendar year

5252.28

Electronic Video of Significant Incidents.

Monitoring video captured and stored in electronic format during facility daily operations where a significant or catastrophic event occurs, such as but not limited to, criminal activity, fire, accidents, natural disasters, etc.; or which an event has been identified at the time as having possible legal, safety, political, or media implications which is stored or saved before automatic deletion of continuous loop video capturing system.

*NOTE – Above schedules are applicable at this time; in the future Knightscope K5 may need its own Record schedule.

The NARA retention Schedule can be found here. nara-records-schedule-list.pdf (archives.gov)

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.

This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes.

3.3b Please indicate each records retention schedule, series, and disposition authority?

VHA RCS 10-1 Item # 5252.10 Chapter 5, 5252 Police Records Items 5252.9, 5252.10, and 5252.28

Records of Routine Security Operations – VHA RCS 10-1 Item# 5252.9

Records about detecting potential security risks, threats, or prohibited items carried onto Federal property or impacting assets, including records documenting access control, screening, patrol and response, and control center operations. Includes:

•surveillance records

•recordings of protective mobile radio transmissions

•video surveillance recordings

•closed circuit television (CCTV) records

NOTE: Records of accidents and incidents are covered under item 100 and records of visitor processing are covered under items 110 and 111.

EXCLUSION: Law enforcement officer-related records, which are covered by agency-specific schedules. Temporary. Destroy when 30 days old, but longer retention is authorized if required for business use. GRS 5.6, item 090 DAA-GRS-2017-0006-0012

Incident transferred to a different record series

Accident / Incident Records – 3 years after final investigations

VHA RCS 10-1 Item# 5252.10

Maintained as an active file based on case being open or closed

Once case is closed – 3-year countdown begins at the end of that calendar year

5252.28

Electronic Video of Significant Incidents.

Monitoring video captured and stored in electronic format during facility daily operations where a significant or catastrophic event occurs, such as but not limited to, criminal activity, fire, accidents, natural disasters, etc.; or which an event has been identified at the time as having possible legal, safety, political, or media implications which is stored or saved before automatic deletion of continuous loop video capturing system.

*NOTE – Above schedules are applicable at this time; in the future Knightscope K5 may need its own Record schedule.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Since the information is being generated by a CCTV based video recorder, the information is written over and physical destruction or remote wiping is not necessary.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Knightscope does not use PII for testing, training, or research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The information maybe retained longer than necessary which could increase the chance of an information breach.

Mitigation: Knightscope collects the following information that can have a risk impact: Email addresses are collected specifically for an authorized user to log into the KSOC (User Interface). It is collected to ensure that only authorized VA users can access the interface. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
We also collect the users name when creating the account. This is done to ensure that the user accessing the system is an authorized VA user. This information is provided to Knightscope by the VA Police representative during new user on boarding. To keep this information safe

Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police can enter the license plate numbers of violators or from other law enforcement agencies. This allows them the ability to identify vehicles on the property that may be related to criminal activity and is used solely for investigative purposes. The information is provided by the VA Police for entry to the system by either Knightscope or an authorized VA Police user. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
Individual users have the option of entering their phone number in the user interface so that they can receive notifications from the KSOC. This is only used by the users that desire this level of notification and the information is provided to Knightscope by the authorized user, or the user can enter the information themselves. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
The Knightscope robots in use capture live video recordings, live audio, and an intercom that records the communications. These onboard tools are used by the VA Police to monitor the area in real time, assess situations remotely using the live audio function (NOT RECORDED) and provide emergency communications to visitors via the intercom. When the intercom is activated, it does broadcast a message stating, “Audio and Video are now being recorded for public safety”. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police also have the option of capturing and receiving notifications of detected devices. Knightscope ASRs can capture the MAC address of Wi-Fi connected devices. This information has been used to identify suspects returning to the scene and gives law enforcement immediate notification that a potential suspect is in the area. Entering the MAC address can be accomplished by a request to Knightscope from an authorized VA user. The VA Police also can enter the device MAC as needed as well. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of the Senior Security Officer VA Police	Used for VA Police purposes, including, evidence collection and case preparation.	Video, license plates, or voice recordings	The evidence gets recorded in a log then gets burned onto a DVD, then logged into a storage facility using the log will stay at storage facility until logged out to be utilized by legal team for case.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Data is shared improperly.

Mitigation: The proper levels of permissions are given to the VA Police personnel and the system is configured to match the FedRAMP security controls. The collected information will only be used in an approved VA Official capacity.
Knightscope collects the following information that can have a risk impact: Email addresses are collected specifically for an authorized user to log into the KSOC (User Interface). It is collected to ensure that only authorized VA users can access the interface. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
We also collect the users name when creating the account. This is done to ensure that the user accessing the system is an authorized VA user. This information is provided to Knightscope by the VA Police representative during new user on boarding. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police can enter the license plate numbers of violators or from other law enforcement agencies. This allows them the ability to identify vehicles on the property that may be related to criminal activity and is used solely for investigative purposes. The information is provided by the VA Police for entry to the system by either Knightscope or an authorized VA Police user. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
Individual users have the option of entering their phone number in the user interface so that they can receive notifications from the KSOC. This is only used by the users that desire this level of notification and the information is provided to Knightscope by the authorized user, or the user can enter the information themselves. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
Facial Recognition is an option available to the VA Police but is not currently in use. The information collected is used for law enforcement purposes and provided by VA Police to Knightscope. The VA Police also have the option of uploading suspect images internally as needed. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
The Knightscope robots in use capture live video recordings, live audio, and an intercom that records the communications. These onboard tools are used by the VA Police to monitor the area in real time, assess situations remotely using the live audio function (NOT RECORDED) and provide emergency communications to visitors via the intercom. When the intercom is activated, it does broadcast a message stating, “Audio and Video are now being recorded for public safety”. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police also have the option of capturing and receiving notifications of detected devices. Knightscope ASRs can capture the MAC address of Wi-Fi connected devices. This information has been used to identify suspects returning to the scene and gives law enforcement immediate notification that a potential suspect is in the area. Entering the MAC address can be accomplished by a request to Knightscope from an authorized VA user. The VA Police also can enter the device MAC as needed as well. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a very low risk. Since the only data captured is a person's image, the low risk is associated with a data breach and the image of the person at the hospital would be outside of a controlled data environment. The only data captured is the person's likeness (video) and their location (filmed in public at a Veteran Affairs Medical Center) .

Mitigation: To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1.The information with each application is categorized in accordance with FIPS 199 and NISTSP 800-60. As part of the categorization any PII is identified.
2.The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3.The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4.Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.
5. In addition the only data collected is the User name, email and phone number if the User opts in.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy

policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes, the Knightscope K5 announces that there is a recording about to happen when they device starts the recording of the Video and Audio.

VA Facilities have signs around the facility that states: Video Surveillance (Video and audio surveillance, including body-worn cameras, are in used on these premises.

Knightscope does not collect email addresses from customers directly. Information about users is provided to Knightscope by the VA so there is an assumption that the VA would let those users know that their email addresses will be used.

Also, when a user logs in to KSOC for the first time they will be presented with the terms and conditions for use as listed at: https://www.ksoc.co/terms of service

Document added to the appendix and as a separate PDF.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

The Knightscope Autonomous Robot patrols collecting Video footage. The only data collected outside of video footage, is provided during the establishment of user accounts, notice covered by the User Agreement. The public is notified via signage that recording is taking place, which is the only form of data collection that takes place, outside of the minimal user information provided during the creation of the User Account.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Knightscope does not collect email addresses from customers directly. Information about users is provided to Knightscope by the VA so there is an assumption that the VA would let those users know that their email addresses will be used.

Also, when a user logs in to KSOC for the first time they will be presented with the terms and conditions for use as listed at: https://www.ksoc.co/terms_of_service

Document added to the appendix and as a separate PDF

The K5 robot tells the people around it before it starts recording video and audio files so notice is being provided properly at the Robot at the site of the VA Police required situation.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Users can decline to provide their emails or names to the VA. For Knightscope we receive this information from the VA.

Users are not obligated to provide phone numbers, that is only if they wish to get notifications to that number.

Users cannot opt-out of video or audio recording because it is a constant video stream used for public safety and emergency situations.

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Individuals consent to use of their email and name when they first log into the system. "They consent to Knightscope having read access to the information; no updates are made.

Users cannot opt-out of video or audio recording because it is a constant video stream used for public safety and emergency situations.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: A person may have information on them collected by video and audio files that could end up accessed improperly.

Mitigation: Knightscope collects the following information that can have a risk impact: Email addresses are collected specifically for an authorized user to log into the KSOC (User Interface). It is collected to ensure that only authorized VA users can access the interface. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.

We also collect the users name when creating the account. This is done to ensure that the user accessing the system is an authorized VA user. This information is provided to Knightscope by the VA Police representative during new user on boarding. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police can enter the license plate numbers of violators or from other law enforcement agencies. This allows them the ability to identify vehicles on the property that may be related to criminal activity and is used solely for investigative purposes. The information is provided by the VA Police for entry to the system by either Knightscope or an authorized VA Police user. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
Individual users have the option of entering their phone number in the user interface so that they can receive notifications from the KSOC. This is only used by the users that desire this level of notification and the information is provided to Knightscope by the authorized user, or the user can enter the information themselves. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
Facial Recognition is an option available to the VA Police but is not currently in use. The information collected is used for law enforcement purposes and provided by VA Police to Knightscope. The VA Police also have the option of uploading suspect images internally as needed. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
The Knightscope robots in use capture live video recordings, live audio, and an intercom that records the communications. These onboard tools are used by the VA Police to monitor the area in real time, assess situations remotely using the live audio function (NOT RECORDED) and provide emergency communications to visitors via the intercom. When the intercom is activated, it does broadcast a message stating, “Audio and Video are now being recorded for public safety”. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.
VA Police also have the option of capturing and receiving notifications of detected devices. Knightscope ASRs can capture the MAC address of Wi-Fi connected devices. This information has been used to identify suspects returning to the scene and gives law enforcement immediate notification that a potential suspect is in the area. Entering the MAC address can be accomplished by a request to Knightscope from an authorized VA user. The VA Police also can enter the device MAC as needed as well. To keep this information safe Knightscope employs an encrypted connection, HTTPS on port 443, and TLS1.2 or greater with no continuing support for later TLS versions.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Knightscope depends on the VA to ensure that the email address and name of users is correct, which is the only data input into the system. Users with User accounts may add their phone number and update that if desirable. No data, other than video, is collected by any person(s) outside of the Users with User accounts.

This video data is being collected in real-time and paints an accurate representation of past events. In the event it is needed for judicial processes it must remain unchanged and in its original format. For this reason, audio and video cannot be corrected and must remain in its original state.

The information is the physical representation of the individual with no identifying or accompanying input, requiring no corrections and/or amendments.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

There is no exemption from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

Requests for provision are covered under general FOIA requests for publicly available video, with the review, input, and redaction requirements of the VHA Privacy Office. The system does not collect PII at the level that is identifiable to unique identifiers, such as name, Date of birth or Social Security Account Numbers of individual customers. As an example, the system does not have the capability to search for individuals by likeness and there isn't a mechanism to distinguish, other than by viewing, one customer from another.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The information is the physical representation on video of the individual with no identifying or accompanying input, requiring no corrections and/or amendments.

Because no data is collected other than the physical representation of a person, there is no data collected to be corrected.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Because the system only stores the individuals likeness, unidentified by any personal identifiers, there isn't a mechanism or information that requires review or potential correction. Additionally, the information must be kept intact in its original format with no changes due to potential use in formal legal proceedings as evidence.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

There are no alternatives to formal redress.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Individuals are unable to retrieve, have access to through the proper VA Channels to have their information corrected in the system.

Mitigation: Data an be accessed by the VA Police Officers using the Knightscope SaaS Solution to help correct any data that is not correct on an Individual using connection that are encrypted, Https port 443, TLS of 1.2 or greater to transmit the Video and Audio files.
-Any video and/or audio that is will be used as evidence is stored with the Evidence Custodian and cannot be altered. It will also follow the 3 year maximum after the case has been adjudicated per VHA RCS 10-1 Item # 5252.10

Section 8. 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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?
User access is provided by the VA Police Department, and they can create new user accounts as needed. Knightscope can support and create new user accounts as well, but it this is only authorized by the representative for the VA Police contacting their direct Knightscope representative where emailed request is the authority to create the account. Individual user permissions are also identified and configured in the same manner.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no Users from other agencies that will have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

There are two roles

Admin: Able to create new user accounts and able to retrieve and preserve data for evidentiary purposes.

User: Has access to the system and is able to retrieve data; however, this information is "view only".

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access

to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, however, the PII is limited to the likeness of generic persons and license plates. There is no PII input that differentiates from one likeness from another.

Contract does not require an NDA. There is no VHA equipment there for this project/program, so no BAA is required.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Knightscope will provide privacy and security training per the Knightscope K5 Robot project implementation. In addition, VA Police will also plan to develop a curriculum through VA Law Enforcement Training Center (LETC) for the Knightscope K5 Robot that will include privacy, security, and accessing PII. Currently VA police officers take courses for already established VA Privacy and Security training offerings. The Knightscope specific privacy and training will be part of the Knightscope K5 Robot Project; that has not yet occurred. LETC training plans will be developed after the police officers associated with the Knightscope K5 project have been trained and project systems is approved to move into production.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Knightscope was granted ATO on December 22, 2023.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, SaaS

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, The Government owns the data.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the

automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No or N/A due to the system does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2024.02.14 11:32:05 -06'00'

Privacy Officer, Lynn Olkowski

SCOTT MILLER

Digitally signed by SCOTT MILLER
Date: 2024.02.14 11:20:06 -05'00'

Information System Security Officer, Scott Miller

SCOTTIE ROSS

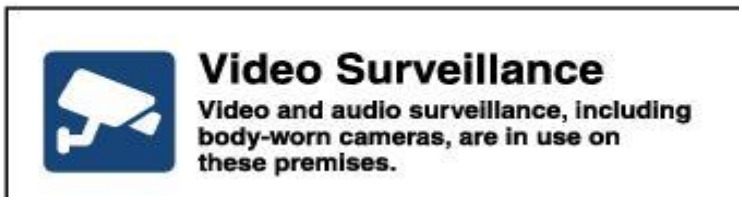
Digitally signed by SCOTTIE ROSS
Date: 2024.02.14 13:53:05 -05'00'

Information System Owner, Scottie Ross

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Required signage at all VA Medical Centers, notifying individuals that Video Surveillance is in use.



HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices