Privacy Impact Assessment
for the

Radio Over IP (ROIP)

DHS/USSS/PIA-022

June 21, 2018

Contact Point
Christal Bramson
Acting Privacy Officer
United States Secret Service
(202) 406-5838

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Secret Service (USSS) Radio over IP (RoIP) system is a Land Mobile Radio (LMR) system, or a secure wireless radio communications system, deployed to provide voice and voice management needs for protective and investigative personnel. USSS RoIP is used by USSS protective details to ensure the security of protectees and protected locations through encrypted communications to and from USSS headquarters. Additionally, USSS uses RoIP for communication during criminal investigations in furtherance of USSS's investigative mission. The USSS is conducting this privacy impact assessment (PIA) because the RoIP system may collect and store personally identifiable information (PII) during the normal course of operations.

Overview

USSS requires a communications system that provides mission critical tactical communications, operational planning, radio network control services, and investigative and protective information communications to support USSS operations and other law enforcement activities. The USSS RoIP system is an internal, encrypted LMR communications system responsible for critical voice and data needs for USSS personnel. The RoIP system transmits and receives (TX/RX) encrypted voice communications to and from USSS Headquarters (HQ). The RoIP system records all audio transmissions through a digital audio logging recorder located at USSS headquarters. The RoIP system may capture PII such as name or physical description in voice communications and subsequently maintain the PII by the digital audio logging recorder for no more than 30 days at USSS HQ. Not all data collected by the RoIP system may be used to identify an individual at the time of collection; however, data captured using the RoIP may later be associated with an individual. USSS is better able to respond to and coordinate its protective and investigative responses to events using RoIP technology, or a secure wireless radio communications system, as described in this PIA. Below are descriptions of the different uses for the RoIP system by the USSS:

Uses

- The RoIP system provides USSS with radio communications supporting security at the White House Complex, the Vice President's residence, the Department of the Treasury (as part of the White House Complex), and foreign diplomatic missions. U.S. Treasury personnel do not have access to the RoIP system.
- Protective details of the agency use RoIP to ensure the security of the President and Vice President and their families, national and visiting world leaders, former Presidents, and events of national significance in the Washington, D.C. area.

- RoIP is used for interoperability between the White House Communications Agency (WHCA) and many other federal, state, and local agencies. There is shared communications between the USSS and WHCA LMR systems. The dispatch units for the respective organizations receive the transmissions. However, the recordings are logically separated, and each agency does not have access to another agency's recordings.
- RoIP may also be used to provide communications while a particular individual or location is being surveilled as part of a law enforcement investigation. The recorded communications may be used as evidence if they became associated with an ongoing law enforcement investigation and official case file. The recorded communications are retrieved by date, location, hours, or channel (frequency band used) during a criminal proceeding and not by personal identifiers.

All USSS personnel with access to the RoIP system are cleared and approved by the USSS Security Management Division (SMD). SMD personnel do not have access to RoIP but process the USSS clearances for personnel who have been granted access. Only personnel assigned to the Radio Branch have the capability to access RoIP audio recordings.

RoIP communications are managed by the Wide Area Virtual Environment (WAVE) system from USSS HQ-managed desktops. WAVE is a commercial software not available to the public. WAVE is accessed through a web-portal interface administered by and restricted to authorized RoIP personnel from computers on the USSS network. Authorized users log on to their computers and are authenticated through the use of two-factor authentication (PIV cards). Authorized users then open a WAVE console on their computer to manage radio communications.

RoIP records radio conversations between USSS personnel in the field and dispatch operators. The USSS uses audio logs to retrace the activity when investigating incidents involving USSS personnel. The recordings are filed and tagged by date and time. The audio files are kept for a period of no longer than 30 days on a USSS recording device, JEI Digital Voice Recorder DVL-FS Series, hosted at USSS HQ. After 30 days, recordings are overwritten by the system unless the information is used in support of ongoing law enforcement investigations through a USSS Court Liaison request by the appropriate federal law enforcement agency or prosecutor. In the event that an audio file is requested to support an ongoing law enforcement investigation, the audio file is transferred to a secondary server where it is housed until the close of the investigation.

Federal and local authorities can also make requests to obtain recordings via a Freedom of Information Act (FOIA) request. Once a request is received, the USSS Uniformed Division will request the recording from the USSS Radio Branch and provide the associated investigative case file number. Once the file is located, it is placed on a DVD and logged via an Audio Records Receipt. The USSS Radio Branch maintains a binder containing a log of all audio file requests. A copy of the initial request and associated Audio Records Receipt is also retained.

All USSS hardware assets are assigned a Secret Service Property Number (SSPN). The physical radios utilized in support of the RoIP system are considered USSS hardware and have SSPN numbers for tracking within the Sunflower Asset Management application. All assets assigned to an individual, including radios, are tracked via Sunflower. The Sunflower application is part of the USSS Travel Manager, Oracle Financials, PRISM, Sunflower (TOPS) system.[1] No RoIP data is input or processed within Sunflower.

Section 1.0 Authorities and Other Requirements

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

USSS investigative and protective functions are authorized by 18 U.S.C. §§ 3056 and 3056A, as well as 18 U.S.C. §§ 871, 879, 1029, 1030, and 1752.

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

Audio recordings made in RoIP are not retrieved using personal identifiers and, therefore, do not constitute a system of records under the Privacy Act of 1974. Recordings from the RoIP system are deleted after 30 days unless the recording is relevant to an active case file for a law enforcement investigation or prosecution. USSS does not associate the recordings with an individual unless the individual is later apprehended or otherwise identified as part of law enforcement investigation. In those instances the recorded communications may be used as evidence if they became associated with an ongoing law enforcement investigation and official case file, and are covered under the Secret Service's Criminal Investigation Information SORN[2] or the Protection Information System SORN.[3]

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

Yes. RoIP is in the process of completing its Authority to Operate (ATO) certification, which includes a System Security Plan. An ATO is expected to be granted pending approval of this PIA.

[1] For more information, *see* DHS/ALL/PIA-053 DHS Financial Management Systems, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-fms-august2017.pdf.
[2] DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011).
[3] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

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

Yes. The USSS RoIP system is covered by NARA-approved retention schedule number N1-087-06-001. The RoIP temporarily retains audio recordings for 30 days and then automatically deletes them on the 31st day unless requested for authorized law enforcement investigations or prosecutions as part of a particular case, significant event, pending or current litigation, or special requests. To the extent the recordings are associated with a case file, the information becomes a part of that file and will be retained for the time period specified in the applicable records retention schedule.

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

Due to the law enforcement nature of this information collection, the information that RoIP collects is not covered by the Paperwork Reduction Act. No information is collected in a standardized format directly from members of the public.

Section 2.0 Characterization of the Information

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

The RoIP system is used for radio communications by the Secret Service's protective details and the Washington Field Office as part of the USSS's protective and investigative mission. In the course of performing these protective and investigative functions, the communications made on the RoIP system may include PII/sensitive PII (SPII), such as when conveying the physical description of a person or attempting to confirm the identity of an individual. Examples of PII/SPII that may be captured in these radio communications include: names, physical descriptions, addresses, drivers' license numbers, license plate numbers, and Social Security numbers (SSN) depending on the situation encountered by USSS personnel.

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

The RoIP system logs all audio transmissions between USSS special agents, officers, and dispatch operators through a digital voice recorder hosted at USSS HQ. Recordings may contain PII/SPII (e.g., name, physical description, SSN), but are not identified or retrieved by PII/SPII. Recordings are identified and retrieved by date, location, hours, and channel.

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

No. The RoIP system does not use information from public or commercial sources.

2.4 Discuss how accuracy of the data is ensured.

Audio logs are kept for a period of 30 days and then deleted by the system unless the information is requested as part of a particular case, significant event, pending or current litigation, or special request. When requested, trained USSS personnel retrieve the pertinent recorded transmission. The recordings are identified and retrieved by date, location, hours, and channel and saved to a write-once, read-many (WORM) DVD. The integrity of audio recordings is ensured through established chain of custody procedures and physical security. The recording device is in a locked room accessible only by authorized individuals via badge access within USSS HQ. Recordings can only be accessed by radio personnel with administrative rights.

If the data is associated with an open investigation, the accuracy of any PII contained in that recording is verified as part of the investigation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that RoIP may capture information about individuals who are not relevant to USSS protective and investigative functions.

Mitigation: The RoIP system records voice communications that occur near USSS protectees, at protected locations, and during authorized investigations and would involve communications for which there is probable cause to obtain information about an individual. All information collected that is not needed to carry out the Agency's mission is discarded after 30 days. The USSS retains recordings from the RoIP system only when they are relevant to a particular case, significant event, pending or current litigation, or special requests. Additionally, USSS does not associate the recordings with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation. In those instances the recordings would become part of an official case file, and are covered under the Secret Service's Criminal Investigation Information and System of Records,[4] or the Protection Information System of Records.[5]

[4] DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011).
[5] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

Privacy Risk: There is a risk of over collection of information thought to be relevant to an investigation.

Mitigation: This risk is partially mitigated. Secret Service provides training to personnel in collecting and retaining only information that is necessary to validate identification and carry out the Agency's mission. If information is later determined to not be germane to an open investigation, the associated audio file is deleted after 30 days.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The RoIP system, as an LMR, is used to enable USSS personnel to conduct protective and investigative functions while mobile. The system is used for communication purposes to request information about a subject, such as names, physical descriptions, addresses, driver's license numbers, SSNs, and other information depending on the circumstance. During an encounter with a subject, USSS personnel will use the radio to contact dispatch to request additional information on the individual. The information obtained is used to identify an individual or to describe a person in the course of agency protective, investigative, and law enforcement functions.

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

No.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a potential risk of unauthorized access, use, or disclosure of audio recordings from RoIP.

Mitigation: Access to RoIP recordings is limited to those specific USSS employees (personnel of the Radio Branch) that must use the system as part of their assigned duties. Equipment use is tracked and monitored for accountability. Authorized users and system administrators are the only individuals with access to the system and recordings. All equipment and archives are stored in secure facilities with restricted access. USSS does not share the information with any other component or agency unless it is associated with a particular case,

significant event, pending or current litigation, or special request. When linked to a USSS case, the recordings become part of an official case file, and are covered under the Secret Service's Criminal Investigation Information SORN,[6] or the Protection Information System SORN.[7] Information sharing complies with the routine uses of the respective SORNs.

Section 4.0 Notice

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

In addition to this PIA, the DHS/USSS-004 Protection Information Systems and DHS/USSS-001 Criminal Investigation System SORNs provide general notice regarding the collection of information and how USSS may share the information collected. Additionally, if the information is obtained by the agent or officer directly from an individual, that individual will be aware that the agent or officer is collecting that information. Advanced notice of the collection of information to investigative targets or others involved in an investigation generally is not provided as it would compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings.

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

USSS does not provide opportunities for individuals to consent to, decline, or opt out of the project because doing so could compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings. However, if a witness or subject is asked for information, they may decline to interact with USSS or answer questions.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: The recorded radio communications may include information about an individual(s) later determined to be unrelated the Agency's mission and who were unaware their information was being recorded.

Mitigation: This risk is partially mitigated. An individual that provides information directly to an agent or officer will be aware that the information is being collected. Due to the nature of the law enforcement activity being performed, not all individuals can be given notice of data collection. Furthermore, individuals may not be aware of conversations recorded using this system that may involve their information; in such cases, USSS cannot provide timely notice. This

[6] DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011).
[7] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

PIA serves as public notice of the existence of the RoIP system in support of the Secret Service's missions and that communications over the RoIP system are recorded. Recordings that do not become associated with investigative case files or other actions are automatically deleted after 30 days.

Section 5.0 Data Retention by the project

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

The RoIP temporarily retains audio recordings for 30 days and then automatically deletes them on the 31st day unless requested for authorized law enforcement investigations or prosecutions as part of a particular case, significant event, pending or current litigation, or special requests. To the extent the recordings are associated with a case file, the information becomes a part of that file and will be retained for the time period specified in the applicable records retention schedule; USSS Records Control Schedule NC1-087-84-01 states information that is collected that becomes part of an investigative case file will be retained as a component part of that file for a period which corresponds to the specific case type developed. DHS is currently developing an Enterprise Records Disposition Schedule that will standardize retention across all components for this type of information; and when approved, USSS will adopt and adhere to the retention provisions of that new Enterprise Schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that audio recordings may be retained by RoIP for a longer period than is required for the purpose for which the audio file was collected.

Mitigation: All data recorded by the RoIP system that does not warrant further Agency actions is overwritten automatically after 30 days per NARA retention schedule N1-087-06-001. Audio files that are associated with a case file become a part of that case file and are retained for a prescribed period of time in accordance with the appropriate established records retention schedule. Audio files are not identified by and cannot be retrieved with a personal identifier, unless they become part of a case file.

Section 6.0 Information Sharing

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

No. Normal RoIP operations do not provide for sharing of voice recordings with outside agencies. Upon request of an appropriate law enforcement agency or prosecutor's office, the USSS

will make a copy of a recording associated with a particular case, significant event, pending or current litigation, or special requests in furtherance of an investigation or prosecution if the recording is still available. After 30 days, the recording is deleted and cannot be retrieved. Recordings that become part of an investigative case file may be shared on a need-to-know basis with federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities in accordance with the routine uses outlined in the applicable SORNs. The RoIP system does not create files or any documents that link to recorded audio. Recordings are not identified or retrieved through use of PII/SPII.

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

RoIP does not maintain data that is retrieved through use of PII/SPII, and therefore RoIP is not subject to a SORN. For recordings that are associated with an open case file, routine uses in the DHS/USSS-004 Protection Information Systems and DHS/USSS-001 Criminal Investigation System SORNs specifically authorize the disclosure of information on a need-to-know basis to federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities in certain situations relevant to the USSS mission. The information within RoIP is collected and shared only for law enforcement purposes.

6.3 Does the project place limitations on re-dissemination?

Yes. USSS shares audio from the RoIP system only when requested as part of a particular case, significant event, pending or current litigation, or special request. Dissemination to authorized recipients is necessary to further criminal investigations or to support protective operations.

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

Audio files that are shared outside of the USSS are tracked through a log book of all requests received. In addition, an audio recording file receipt is completed by the recipient of the audio file. The form includes the date, nature, purpose of each disclosure, and the name and address of the individual agency to which disclosure is made. Requests for disclosure must be approved by the Program Director and are documented locally.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that audio containing PII/SPII may be disclosed to an unauthorized recipient.

Mitigation: This risk is partially mitigated. When making the call to dispatch, it is possible that bystanders could overhear the information being relayed. Outside of this instance, USSS limits

disclosure of information to only law enforcement agencies and prosecutors' offices when requested. USSS does not use recordings to identify an individual, but instead to complete law enforcement investigative and protective duties. In those instances, the Radio Branch personnel may only share this information pursuant to the routine uses specified in the Secret Service's Criminal Investigation Information SORN,[8] or the Protection Information SORN.[9]

Section 7.0 Redress

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

Conversations recorded by the RoIP system are not generally subject to the provisions of the Privacy Act of 1974 because the recordings are not retrieved by personal identifier. To the extent the recordings become part of the Agency's case files, the procedures for access are stated in the SORNs for the applicable systems of records: DHS/USSS-001 Criminal Investigation Information and DHS/USSS-004 Protective Information. USSS investigative and protective records are exempted from the Privacy Act's notification, access, and amendment provisions. However, in those instances in which records become part of an investigative case file, U.S. citizens and Lawful Permanent Residents seeking access to any information contained in RoIP, or seeking to contest its content, may submit a request in writing to the USSS Freedom of Information Act/Privacy Act (FOIA/PA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223, as specified in the applicable SORN. Individuals, regardless of citizenship or legal status, may request access to their records under FOIA. Notwithstanding the applicable exemptions, USSS reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with, or adversely affect the accomplishment of the Secret Service's protective and investigatory mission, information may be released or amended.

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

Conversations recorded by the RoIP system are not subject to the amendment provisions of the Privacy Act of 1974, as they are not retrieved through the use of a personal identifier, and, may be exempt from the Privacy Act's access and amendment provisions. In instances in which records become part of an investigative case file, correction of information is outlined in the SORNs associated with those files. The applicable SORN notifies individuals how to correct their information. USSS will review each request and grant amendment on a case-by-case basis.

[8] DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011).
[9] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

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

Conversations recorded by the RoIP system are not subject to the notification provisions of the Privacy Act of 1974 as they are not retrieved through the use of personal identifiers. Notice that records in this system may be exempted from the access and amendment procedures of the Privacy Act is outlined in this PIA in Sections 7.1 and 7.2. In instances in which records become part of an investigative case file, correction of information is outlined in the SORNs associated with those files.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is the risk individuals may have their information erroneously associated with a crime without the ability to correct it.

Mitigation: USSS does not use recordings to identify an individual, but instead to complete law enforcement investigative and protective duties. An individual may contest the association with a particular recording during the course of the subsequent criminal proceeding if he or she is erroneously associated with the recording. As stated above, in those instances in which records become part of an investigative case file, correction of information is outlined in the SORNs associated with those files.

Section 8.0 Auditing and Accountability

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

Only authorized users have access to the files recorded in the system. The files can be identified only by date, location, hours, and channel on which the recording took place. RoIP provides a copy of pertinent audio files only when requested internally or by an appropriate law enforcement agency or prosecutor's office to support an investigation or open case. Any requests are routed through the USSS Office of Chief Counsel and USSS Privacy Office for review. Any shared recording is logged with the same date, location, hours, and channel data before being released to an authorized individual for transport to the requesting authority.

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

All USSS personnel undergo initial security awareness training and complete the DHS security awareness and rules of behavior training course and a privacy awareness course on an

annual basis. In addition, system specific paper-based (booklet form) training is provided by vendors for specific equipment and applications, and is shared by all users.

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

Only personnel cleared by the USSS Security Management Division (SMD) and assigned to the Radio Branch have the capability to access audio recordings.

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

The RoIP system does not have existing or planned Memoranda of Understanding or information sharing agreements. Audio segments are only provided to law enforcement agencies or prosecutor's offices as part of legal investigations or prosecutions upon request. Access to the system is not available to anyone not identified in Section 8.3.

Responsible Official

Christal Bramson
Acting Privacy Officer
United States Secret Service
Department of Homeland Security

Approval Signature

[Original signed and on file at the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security