

# Privacy Impact Assessment

for

## Natural Resources and Environment FS Voice over IP (NRE FS VoIP)

Policy, E-Government and Fair Information Practices

Version: 1.5

Date: August 15, 2022

Prepared for: USDA OCIO-Policy, E-Government and Fair Information  
Practices (PE&F)





## **Contact Point**

Zahid Chaudhry

System Owner

USDA NRE Forest Service

503-808-2440

## **Reviewing Official**

Cynthia Towers Ebersohn

Privacy Officer

USDA NRE Forest Service

386-301-4060

## Abstract

Voice over Internet Protocol (VoIP), also called IP telephony, is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN), also known as plain old telephone service (POTS). The NRE FS VoIP is the Voice over IP system for enterprise level voice services and messaging for USDA Forest Service. Call center managers are located in Springfield Oregon and Albuquerque New Mexico for redundancy.

## Overview

The Forest Service (FS) of the United States Department of Agriculture (USDA) is a multi-faceted agency that manages and protects 154 national forests and 20 grasslands in 44 states and Puerto Rico. The agency's mission is to sustain the health, diversity, and productivity of the nation's forests and grasslands to meet the needs of present and future generations.

The NRE FS VoIP is the Voice over IP system for enterprise level voice services and messaging for USDA Forest Service. Call center managers are located in Springfield Oregon and Albuquerque New Mexico for redundancy. Forest Service users communicate over the FSCB Network to transmit and access personalized and messaging data from Forest Service VoIP call and unity managers providing voice and messaging services.

Principal system components consist of four CISCO servers running CISCO Unified Communication Operating System (UCOS). Hard Phone / Physical handsets consist of CISCO, Polycom and V-Tech devices.

This PIA is being created for NRE FS VoIP. This privacy impact assessment identifies how information about individuals is handled within NRE FS VoIP in accordance with OMB M-03-22.

## Section 1.0 Characterization of the Information

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

### 1.1 Identification

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

FS NRE VoIP is a Voice over IP telephone system that provides phone and voice mail services. The only information that may contain PII are voice mail messages left by individuals calling Forest Service employees that utilize this phone system.

### 1.2 Source

What is the source(s) of the information in the system?

Voice mail is the only source of information that can be left in the system that may potentially contain PII.

### 1.3 Justification

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

The principal purpose for the voice mail system is the conveying of stored telecommunications voice messages.

### 1.4 Collection

How is the information collected?

The voice messages are saved into a central repository maintained in a Unity server located in Albuquerque, NM with a backup in Springfield, Oregon.

### 1.5 Validation

How will the information be checked for accuracy?

Voice mail messages system allows the person leaving the message to check their messages and either erase and start over or then save the message.

## 1.6 Authority

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

The legal authority to operate the system comes from Executive orders 10450, 10577, 12968, 12968; 5 CFR Parts 5, 731, 732, 736; Title 5 USC Chapters 29, 33, 83, 84, 87, 89, 91. For additional Federal requirements for the collection of information, also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Sched

## 1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

NRE FS VoIP does not collect data, however it is possible that voice mail stored within NRE FS VoIP could contain PII. This content is protected through various levels of security and policy. It is recommended that all VoIP Users post a voice message similar to the following to minimize the possibility for collecting any PII:

"You have reached the voice mail of <name>. Please leave me your name and phone number and I will return your call as soon as possible. As a reminder, do not leave any personal information such as your social security number or medical information. I will gather any necessary personal information when I return your call. Thank you."

## Section 2.0 Uses of the Information

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

### 2.1 Usage

Describe all the uses of information.

NRE FS VoIP is a Voice over IP telephone system that provides phone and voice mail services. The principal purpose for the voice mail system is the conveying of stored telecommunications voice messages.

### 2.2 Analysis and Production

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

Real Time Monitoring Tool- Data Produced is raw audit data used to troubleshoot and monitor events or alerts

### 2.3 Commercial/Public Use

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

Not Applicable- NRE FS VoIP does not use commercial or publicly available data.

### 2.4 Risk Mitigation

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

The content in NRE FS VoIP is protected through various levels of security and policy. The system itself is protected by access layers and positive identification techniques to ensure that only people authorized to view and act upon information can do so. User roles are outlined within the NRE FS VoIP Roles, Responsibilities, and Least Privilege Table. Organizational user accounts are created and authenticated via username and password. Voice mail access is protected by authentication by PIN number.

## Section 3.0 Retention

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

### 3.1 Time Period

How long is information retained?

Voice messages within the NRE FS VoIP can be retained indefinitely for up to 14 MB of storage per user. The number of messages retained within the 14 MB is dependent on the size of the messages stored. If the 14 MB storage limit is reached, the system will not retain additional voice messages for that user. Deleted voice messages are retained for 15 days.

### 3.2 Approval

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

NRE FS VoIP abides by the FS and the Federal Government's policies regarding the record retention policies for legal contracts and similar documents. Records Officer can be contacted for additional records information as required.

### 3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risks are low on the retention period of the potential data that is stored in the form of voice mails. The retention period is controlled by the owner of the voice mail box and is based on personal requirements for each user. These are mitigated by each user setting a unique pin which is required to access data stored in the voice mail storage. Once a voice mail is deleted there is a default 15-day retention before the voice mail is permanently deleted by the system.

## Section 4.0 Internal Sharing and Disclosure

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

### 4.1 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

Not Applicable – NRE FS VoIP does not share information with external organizations.

### 4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Not Applicable – NRE FS VoIP does not share information with external organizations.

### 4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Not Applicable – NRE FS VoIP does not share information with external organizations.



## Section 5.0 External Sharing and Disclosure

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

### 5.1 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

Not Applicable – NRE FS VoIP does not share information with external organizations.

### 5.2 Compatibility

Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN?

**If so**, please describe, provide SORN name and hyperlink URL to text.

**If not**, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Not Applicable – NRE FS VoIP does not share information with external organizations.

### 5.3 Delivery and Security Measures

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

Not Applicable – NRE FS VoIP does not share information with external organizations.

### 5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not Applicable – NRE FS VoIP does not share information with external organizations.

---

## Section 6.0 System of Records Notice (SORN)

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

### 6.1 Requirement and Identification

Does this system require a SORN?

**If so**, please provide SORN name and hyperlink URL to text.

**If a SORN is not required**, answer “No” to this question, and “N/A” for questions 6.2 through 6.5.

Not Applicable - No SORN is required.

### 6.2 Individual Notification

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

Not Applicable - The system does not collect information.

### 6.3 Right to Decline

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

Not Applicable - The system does not collect information.

### 6.4 Right of Consent

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

Not Applicable - The system does not collect information.

### 6.5 Risk Mitigation

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

Not applicable- NRE FS VoIP is a Voice over Internet Protocol telephone system and does not have the capability to provide notice to individuals.

## Section 7.0 Access, Redress and Correction

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

### 7.1 Access

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

Not applicable – NRE FS VoIP is a Voice over IP telephone system and information access is controlled using roles and permission sets. There are no procedures that apply to allowing individuals to gain access to their information. There is no way to search for information on any individual in the system.

### 7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Not applicable – FS NRE VoIP is a Voice over IP telephone system that provides phone and voice mail services. Correction of Voice mails is not possible in the system.

### 7.3 Notification

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

Not applicable - FS NRE VoIP is a Voice over IP telephone system that provides phone and voice mail services. The system does not have the capability to provide notice to individuals.

### 7.4 Redress Alternatives

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

Not Applicable – Individuals calling into the phone system can choose not to leave a voice mail and hang up.

### 7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.



Not applicable - FS NRE VoIP is a Voice over IP telephone system that provides phone and voice mail services. The system does not have the capability to provide notice to individuals.

---

## Section 8.0 Technical Access and Security

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

### 8.1 Procedures

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

Users are granted access to the system based on locations served by the VoIP services as part of the base service required as base services to complete their job functions, System Admins are granted access based on a completed and approved Network Tools Security Agreement.

### 8.2 Contractor Access

Will Department contractors have access to the system?

Yes

### 8.3 Privacy Training

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

All FS staff members are required to complete annual Department Information Security Awareness training. The interactive online training covers topics such as properly handling Sensitive PII and other data, online threats, social engineering, and the physical security of documents and electronics, such as laptops and mobile devices. Individuals with significant security responsibilities (such as Administrators) are required to undergo additional role-based training, tailored to their respective responsibilities.

### 8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer "Yes" and provide ATO expiration date(s).

Yes. ATO expiration date is January 30, 2023.

### 8.5 Audit and Technical Safeguards

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

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 4. This includes at a minimum:

- User identification and authentication
- The use of network and application access controls
- Encryption of data at rest, in transit, and in use
- Auditing of significant changes to systems or data.

Due to the public nature of this document, the method of encryption can be found in the NRE FS VoIP System Security Plan, control SC-13. All encryption is FIPS 140-03 compliant.

## **8.6 Risk Mitigation**

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

NRE FS VoIP does not collect data, it provides telephone and voicemail capabilities. NRE FS VoIP provides security of content while at rest through the access methods and encryption. Files stored in NRE FS VoIP are encrypted while at rest, in transit, or in use in compliance with FIPS 140-3 validated cryptography. The method of encryption can be found in the NRE FS VoIP System Security Plan, control SC-13.

There is minimal risk to the users of the system. The mitigation of risk is handled by making sure that there is limited use and sharing of information, and only to relevant individuals.

NRE FS VoIP will promptly report computer security incidents and breaches affecting FS data/information or systems and promptly coordinate with FS staff on incident handling, response, containment, eradication, and recovery efforts throughout the incident life cycle until fully resolved.

## Section 9.0 Technology

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

### 9.1 Description

What type of project is the program or system?

NRE FS VoIP is a Voice over Internet Protocol Phone system with voicemail feature.

### 9.2 Privacy Concerns

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

No

---

## Section 10.0 Third Party Websites/Applications

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

### 10.1 Review

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

Yes

### 10.2 Purpose

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

Not Applicable

### 10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

Not Applicable

### 10.4 PII Usage

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

Not Applicable

### 10.5 PII Maintenance and Security

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

Not Applicable



### 10.6 PII Purging

Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

Not Applicable

### 10.7 PII Access

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

Not Applicable

### 10.8 PII Sharing

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

Not Applicable

### 10.9 SORN Requirement

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

Not Applicable

### 10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not Applicable

### 10.11 Web Measurement and Customization Opt-In/Opt-Out

Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology? If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Not Applicable

### 10.12 Risk Mitigation

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

Not Applicable



---

## Responsible Official

**Zahid Chaudhry** Digitally signed by Zahid Chaudhry  
Date: 2022.08.15 13:18:46 -07'00'

---

Zahid Chaudhry  
System Owner (SO)  
Natural Resources and Environment, Forest Service  
United States Department of Agriculture

## Approval Signature

**CYNTHIA TOWERS** Digitally signed by CYNTHIA TOWERS  
Date: 2022.08.16 08:25:41 -05'00'

---

Cynthia Towers Ebersohn  
Privacy Officer (PO)  
Natural Resources and Environment, Forest Service  
United States Department of Agriculture

**BENJAMIN MOREAU** Digitally signed by BENJAMIN MOREAU  
Date: 2022.08.16 12:47:29 -04'00'

---

Benjamin Moreau  
Assistant Chief Information Security Officer (ACISO)  
Natural Resources and Environment, Forest Service  
United States Department of Agriculture