U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Integrated Digital Voice Communication System (IDVC)
Bureau/Office: Office of the Chief Information Officer
Date: March 12, 2021
Point of Contact
Name: Vany Kaiser
Title: Departmental Privacy Act Specialist
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

☒ Members of the general public
☒ Federal personnel and/or Federal contractors
☒ Volunteers
☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Integrated Digital Voice Communication (IDVC) System is a general support system that provides analog and digital voice communications technologies to the Department of the Interior (DOI) personnel at the following locations:

- DOI Main Interior Building (MIB) – 1849 C Street, NW, Washington, DC 20240

- Office of the Chief Information Officer (OCIO) and Customer Service Center (CSC) Help Desk – 7301 W. Mansfield Ave. Lakewood, CO 80235
- Office of Hearings and Appeals (OHA) – 801 Quincy Street, Arlington, VA 22203
- Acquisitions Services Directorate (AQD)
    - 354 S HWY 92 Sierra Vista, AZ 85635
    - 318 Elden Street, Herndon, VA
- U.S. Geological Survey (USGS) Headquarters, 12201 Sunrise Valley Dr., Reston VA 20192

The IDVC system is deployed on its own wide area network (WAN). The WAN is physically and logically separated from all DOI data networks and the Internet, providing an extra layer of security. The MIB serves as the central administration point and each of the IDVC locations connects back to the MIB via dedicated T1 circuit.

The IDVC is a closed system and is not connected to any other networks or to the Internet, information remains within the IDVC boundary. The IDVC infrastructure utilizes the OmniAccess routers and OmniStack switches to route information to system components throughout the IDVC network.

The IDVC system is managed and administered by the OCIO Telecom Support Section personnel. The information processed within the IDVC includes DOI employees' names, office phone numbers, outside phone numbers, call duration, and voicemail messages.

C. What is the legal authority?

31 U.S.C. 1348(b), 44 U.S.C. 3101, 44 U.S.C. 2904 and 44 U.S.C. 2906

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name:*

UII code: 010-000000357; Integrated Digital Voice Communications System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
OmniVista 8770	Administration PC	Yes	The OmniVista 8770 is the administration console for the phone system. The 4760 contains user's profiles that consists of phone number assignment and profile features such as call forwarding to personal phones or assistants, as well as call log information.
AVST Call XPress	Voicemail server	Yes	This software provides centralized management of the automated attendant feature, as well as voicemail mailboxes. Phone number, names, and call forwarding are PII.
OmniTouch Contact Center Software (CCS) aka (Genesys)	Call Routing solution. Contact Center	Yes	Provides inbound voice, agent desktop, and real-time and historical reporting infrastructure for the Customer Support Center (CSC). Phone number, names, and call forwarding are PII.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI-36, Telephone Call Detail Records, 59 FR 7260 (February 15, 1994), modification published at 73 FR 8342 (February 13, 2008) which may be viewed on the DOI SORN website at:

https://www.doi.gov/privacy/doi-notices. This SORN is being revised to update all sections and incorporate recent Federal policy in accordance with OMB Circular A-108.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Home Telephone Number
☒ Other: *Specify the PII collected.*

Other personal information may be provided by individuals through voice mail. IDVC system administrators and technicians are required to log on to the IDVC system with a unique user identification and password.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☐ Web site

☐ Fax
☐Telephone Interview
☐ Information Shared Between Systems
☒ Other: *Describe*

Head Quarters (HQ)Telecom Support Section receives a customer request in Remedy ticketing system. A Telecom technician inputs the new user’s first and last name and assigns an available telephone number using the OmniVista 8770 administration console and a voicemail port using Call Xpress.

D. What is the intended use of the PII collected?

The intended use of the PII is to create a firm record of in/out-bound calls and voicemail on the telephone network. This use is consistent with the published SORN.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Users with access to the phone network may utilize the dial-by-name directory to search for employees. Information may be shared within the DOI to determine responsibility for long distance telephone calls, and to resolve disputes and facilitate the verification of discrepancies relating to the billing, payment, or reconciliation of telephone operational or accountability records. PII is shared with an OCIO Telecom technician to enter the new user’s name into the system and assign an available telephone number and a voicemail port.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Users with access to the phone network may utilize the dial-by-name directory to search for employees.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Any individual may contact the DOI Internal Operator (switch board) and be transferred to phone network users. Information may be shared with other Federal agencies for an authorized purpose as outlined in the DOI-36 SORN.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with representatives of a telecommunications company providing telecommunications support to permit the servicing of the account as authorized by DOI-36 SORN.

☒ Other Third-Party Sources: *Describe the third party source and how the data will be used.*

Information may be shared with third parties as covered under the routine uses in the DOI-36 SORN.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

DOI employees are assigned a phone number to conduct official business and may not have opportunities to consent to the use of their name and assigned numbers to determine responsibility for telephone calls, resolve disputes and facilitate the verification of discrepancies relating to the billing, payment, or reconciliation of telephone operational or accountability records. As this is a Government IT System, all users are subject to applicable usage and monitoring policy and consent to such monitoring by acknowledging rules of behavior when accessing DOI network assets.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the published DOI-36 SORN.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records are retrieved by employee name, telephone number, identification number, or by account code.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Call detail reports are available to supervisors only and must be formally requested in writing to the HQ Telecom Support Section Chief. Designated system administrators will have access to these reports. The reports will be used for the following purposes:

- To review calling patterns and identify possible misuse and abuse of long-distance telephone services.
- To troubleshoot problems with the system.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

DOI receives a monthly bill from the local service provider (Verizon). These records are verified by Designated Agency Representative (DAR) on a monthly basis to ensure billing and profile accuracy.

B. How will data be checked for completeness?

The DAR compares carrier quarterly reports to those of the OmniVista 4760. This process of data comparison ensures both external and internal systems are reporting complete data.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The DAR compares carrier quarterly reports to those of the OmniVista 8770.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Operational system records (Management and Maintenance) are classified under DRS 1.4A(1) (DAA-0048-2013-0001-0013), which was approved by the National Archives and Records Administration (NARA). The records disposition is temporary, and records are retained for no more than 3 years.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal risk to individual privacy for the use of employee name and official phone number. Risk may result from the contents of voice mail that includes personal information; however, this risk is mitigated by employee use of a passcode to retrieve their voicemail. In some cases, employees may forward calls from their official phone number to their personal phone number. This information is included in the Department's monitoring of the system and reports on phone usage. IDVC is a private phone system with implemented access controls. Only authorized technicians are allowed to make changes to the system. Additionally, only the System Administrator may generate Call Detail Records. Call Detail Records contain information about incoming and outgoing calls placed to a specific number, the duration of the call, date, and time of the call. The Section Chief must approve all Call Detail Reports.

IDVC as a FISMA moderate system that requires management, operational, and technical controls established by National Institute of Standards and Technology (NIST) SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII. All DOI employees and contractors complete initial and annual information security and privacy training, and sign DOI Rules of Behavior. Role-based privacy and security training is also required for personnel with privacy or security responsibilities.

The Department utilizes a combination of technical and operational controls to reduce risk in the IDVC environment, such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies. OCIO technicians must have a DOI account and government issued personal identity verification (PIV) card to access IDVC. Bureaus and offices utilizing IDVC are responsible for implementing adequate controls to safeguard PII used or maintained within their environment as appropriate. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the IDVC environment, which will help the agency effectively maintain a good privacy and security posture for the system. The system privacy plan outlines the privacy controls and is reviewed annually to ensure adequacy of controls implemented to protect data.

In addition, IDVC employs a variety of management, operational and technical security controls. Administrative access to IDVC is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual security and privacy awareness training, security and privacy role-based training, records, Controlled Unclassified, and Section 508 training in order to obtain and maintain IDVC administrator access.

There is a risk that IDVC system administrators may be able to view files, or folders when access is mistakenly or unknowingly shared by the user. Users of IDVC must take proper precautions when setting access permissions to ensure only those with a need to know are granted access.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. This risk is mitigated by maintaining records in accordance with NARA approved records schedules under DRS 1.4A(1) (DAA-0048-2013-0001-0013). The records disposition is temporary and are retained for no more than 3 years. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

There is a risk users may not have adequate notice of the collection and use of their data. This is mitigated through publication of this PIA and the DOI-36 SORN. These notices provide information to individuals on how their PII will be used and shared and how they may seek notification, access, or amendment of their records.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The phone network allows for communication within and outside the Department for the conduct of official agency business, as well as calling emergency services.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

No new data is collected.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☐ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Users do not have access to the data in IDVC. Their access is limited to basic phone features such as setting up call forwarding and voicemail.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to the data is determined by the requirements associated with their professional responsibilities based on the concept of least privilege rule. IDVC system administrators are required to log on to the IDVC system with a unique user identification and password. All users with logon credentials will be audited. All telecommunications service technicians with logon credentials will be audited.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The IDVC contract contains a Privacy Act clause and Non-Disclosure Agreement clause was included as part of the statement of work and the contractor was provided with DOI's privacy policies.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*
☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

IDVC is not intended to be used to monitor individuals. At the authorization of the Section Chief, the System Administrator has the ability to pull Windows logs to determine the technician's username, logon date, time and user actions on the OmniVista 87700.

M. What controls will be used to prevent unauthorized monitoring?

Access to administrative functions is strictly controlled and can only be granted based on the user's role and responsibilities. The system has access controls and is monitored for authorized and appropriate use. Call Detail Reports are generated and reviewed. All DOI employees and contractors complete initial and annual information security and privacy training, and sign DOI Rules of Behavior.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

Chief, Enterprise Infrastructure Services within the Office of the Chief Information Officer serves as the IDVC Information System Owner and the official responsible for oversight and management of security controls and the protection of agency information processed and stored in IDVC. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in IDVC, in consultation with the Departmental Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The IDVC Information System Owner and Information System Security Officer is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The IDVC Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with Federal policy and DOI policy and procedures outlined in the DOI Privacy Breach Response Plan.