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: MobiKEY
Bureau/Office: United States Fish and Wildlife Service (FWS)
Date: June 30, 2017
Point of Contact
Name: Peter Bonora
Title: FWS/IT Specialist
Email: peter_bonora@fws.gov
Phone: (703) 358-2167
Address: 5275 Leesburg Pike, Falls Church, VA 22041

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?

MobiKEY is a minor application within the Enterprise Core Network Services (ECNS) system, a U.S. Fish and Wildlife Service (FWS) General Support System (GSS), that supports secure remote access for FWS personnel. MobiKEY is a secure remote access system that uses two factor authentication to allow FWS users to remotely access their authorized FWS Government Furnished Equipment (GFE) workstation, or GFE Virtual computer, from any Internet-enabled PC, MAC computer, or iPad that are running at a government facility. The MobiKEY software is on a universal serial bus (USB) device, and when executed on a remote computer, works in conjunction with an Internet connection, the Defense

Identity Management Network (DEFIMNET) infrastructure, and the MobiNET agent running on a user's host computer.

MobiKEY allows authorized users to securely view and control the host computer's desktop and applications, while providing access to FWS network services as though the user was in the office. All files stay on the host computer securely in the defense enclave. Only mouse, keystroke, and screen information is exchanged, no information can be printed or downloaded to the remote computer. The host computer is not available for use locally during the remote session as the keyboard, mouse, and monitor are disabled. The MobiKEY solution requires the remote computer to have an Internet connection and the host computer must be turned on and connected to the FWS/DOI network.

C. What is the legal authority?

- Departmental Regulations, 5 U.S.C. 301;
- The Paperwork Reduction Act, 44 U.S.C. Chapter 35;
- The Clinger-Cohen Act, 40 U.S.C. 1401;
- Office of Management and Budget Circular A-130, Management Information as a Strategic Resources
- Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011;
- Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; and
- Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

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: UII Code: 010-000001849; System Security Plan (SSP) for MobiKEY
☐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.*
None	Not Applicable	Not Applicable	Not Applicable

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)*
☒No
MobiKEY is not a Privacy Act system. User network credentials and Active Directory records are maintained under DOI-47, Logical Security Files, 72 FR 11040, March 12, 2007

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
☒Other: User name, User Principal Name (UPN), PIV credentials, Work email addresses of all FWS employees and contractors who use MobiKEY for remote access. Audit logs collect user activities: date; start and end time; duration of session; connection type; MobiNET ID; Smart card serial number; remote global ID; remote IP address; host global ID; host name; host IP address; host owner.

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: Users call MobiKEY Support when they first register and activate their accounts. This is a one-time event and the MobiKEY Support person requests the user's UPN information to associate their PIV card credentials with their MobiKEY account. The only user information stored at enrollment time is First/Last Name, Email Address and User Principal Name (UPN). The Electronic Serial Number of the MobiKEY device that is used to complete the registration is also stored. Active Directory is not accessed directly. The UPN itself is not stored, but rather only the hash of the UPN.

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

User PII is used to provide secure remote access to their agency host computers. The user information is used during initial user account registration and activation to associate a person with their PIV credentials/certificate. Once that occurs, all authentication is verified via certificates and no PII is collected.

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.*
MobiKEY is strictly an authentication tool that uses two factor authentication to connect a remote system to a designated FWS system. Any PII associated with its use is contained in audit logs and is only accessible by system managers for periodic review or troubleshooting.

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

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

☐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.*
Contractors provide support to FWS for managing, processing, and troubleshooting in MobiKEY.

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

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.*

Use of MobiKEY devices is voluntary and users have the opportunity to decline providing their information by not registering for a MobiKEY account. However, MobiKEY users are required to provide their name and email address to register and to authenticate their identity to remotely access the FWS environment. This information is required to ensure network security during the use of MobiKEY. If the user does not provide their name and email address to register for a MobiKEY account, then the user will not be authorized to use the system.

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

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: Notice on information practices for MobiKEY is provided through the publication of this privacy impact assessment.

☐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.).

The system retrieves name, username, email address, and UPN when a MobiKEY account is initially registered. Following the initial registration, the user will be required to access the system using their PIV card and certificate for authentication in order to start a MobiKEY session.

I. Will reports be produced on individuals?

☒Yes: *What will be the use of these reports? Who will have access to them?*
MobiKEY will produce reports on audit logs that collect the following: username, the specific working desktop being accessed, result of the operation (granted/denied), time and date of the access, length of time system is accessed, network information about both user location and the desktop location. These audit logs are only accessible to the MobiKEY security audit committee and reviewed on a quarterly basis.

☐No

Section 3. Attributes of System Data

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

The MobiKEY system does not collect data from sources outside of the DOI. Only authorized users with current and accurate credentials, active authorized PIV card, and a valid and authorized MobiKEY account can access MobiKEY.

B. How will data be checked for completeness?

The DOI Enterprise Active Directory system will authenticate the user's "username" and credentials when the user logs into the DOI network, and these usernames and credentials are kept current by the AD system. If the user does not have a valid, authorized MobiKEY account they cannot perform any activities within the system.

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

MobiKEY usernames and email addresses are kept current by updates to the DOI Enterprise Active Directory system, which is managed by the AD Administrators.

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

Retention periods for records created and accessed by MobiKEY users may vary, as records are maintained by subject matter in accordance with the applicable Departmental or FWS records schedule, or General Records Schedule.

Records relating to user identification, authorizations, audit trails, and system maintenance are retained in accordance with a Departmental Records Schedule (DRS) - 1, Administrative Bucket, which has been approved by the National Archives and Records Administration (NARA). The disposition for Short-term Administration Records and Information Technology records is temporary. Records are cut off upon expiration, or when superseded or obsolete as appropriate, and destroyed 3 years after cutoff. (DRS 1.1A DAA-0048-2013-0001-0001 and DAA-0048-2013-0001-0013).

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 384 Departmental Manual 1.

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 privacy of individual MobiKEY users as only the minimum PII required is collected to authenticate users and ensure the security of Federal government data, information systems, and networks in alignment with Federal law, policy and standards. MobiKEY provides secure remote access to authorized FWS workstation, or virtual computer, or user's host computer within the agency environment. MobiKEY allows authorized users to remotely view and control the host computer's desktop and applications securely. The remote print and download functions have been removed from the FWS MobiKEY, so all files stay on the host computer securely in the defense enclave. Only mouse, keystroke, and screen information is exchanged.

Any privacy risks are mitigated by the strict privacy and security controls implemented to ensure the confidentiality, integrity, and availability of the system. The MobiKEY system has undergone a formal Assessment and Authorization and has been granted an authority to operate (ATO) in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. MobiKEY is rated as FISMA moderate and requires strict security controls to protect the confidentiality, integrity, and availability of the data contained in the system.

MobiKEY provides a personal identity and authentication service and creates a secure, encrypted session that is in compliance with Federal security policies. MobiKEY users must have a valid and authorized DOI Enterprise Active Directory account. Separated employees are removed from Active Directory, which effectively removes individual access to the DOI network and to MobiKEY.

MobiKEY is a secure, multi-factor authentication, remote access system that enables a user to access either their FWS GFE PC, or GFE Virtual PC, via Internet-enabled PC, MAC computer, or iPad (any computer with a USB port or lightning connector, including public or personally owned devices). The system only uses PII (name, username, and email address) at the time a user is initially registered to associate the person's PIV card to their MobiKEY account. The data is stored in encrypted, hashed, format on the DEFIMNET authentication server that is located within the DOI network. After initial MobiKEY registration, there is no sharing or transfer of PII during use of MobiKEY to access GFE devices, as MobiKEY uses certificates that are specific to the PIV card and DEFIMNET system to authenticate user identification.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail will include the identity of each user accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. The MobiKEY system follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training and sign DOI Rules of Behavior.

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: The MobiKEY system enables secure remote access by authorized users to their systems within the DOI/FWS network utilizing multi-factor authentication.

☐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?

MobiKEY does not derive new data.

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*

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

Users must complete and obtain their manager's approval of the MobiKEY request form in order to obtain MobiKEY access.

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. The contract between FWS and the vendor contains the FAR clauses for Privacy, including 52.224-1 and 52.224-2.

☐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. The MobiKEY system does maintain system access and audit logs to reconstruct security relevant events. These logs are only accessible to system administrators with elevated privileges.

☐No

L. What kinds of information are collected as a function of the monitoring of individuals?
The audit logs include the identity of each user accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls.

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

FWS fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. Access to MobiKEY audit logs and audit tools are restricted to authorized personnel only via access control lists and authorized access to the MobiKEY dashboard. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The MobiKEY system follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. All employees and contractors are required to complete security, privacy and records management training and sign DOI Rules of Behavior before being granted access to any DOI IT resource, and annually thereafter. Monitoring of MobiKEY users will not extend beyond the access to audit logs that are granted to system administrators on a limited basis.

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. The MobiKEY device requires use of PIV card. The MobiKEY authentication server (DEFIMNET) is housed within the DOI data center located at the USGS facility in Reston, VA. The facility itself is has security guards and requires PIV credentials with approved access rights, to enter. The Data Center itself requires another level of approval and access rights to enter.

(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. The MobiKEY authentication server (DEFIMNET) is subject to all system administration best practices, and all hardware and data is built with "high availability" capabilities (e.g., redundant hardware, software, etc.).

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.

The FWS Deputy Associate Chief Information Officer serves as the MobiKEY Information System Owner and the official responsible for oversight and management of the MobiKEY security and privacy controls and the protection of agency information processed and stored in the MobiKEY system. The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies, and for responding to privacy complaints.

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 MobiKEY Information System Owner is responsible for oversight and management of the MobiKEY security and privacy controls, and for ensuring to the greatest possible extent that data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC, the Department's security incident reporting portal, and appropriate agency officials within 1-hour of discovery in accordance with Federal policy and established procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the FWS Associate Privacy Officer.