Privacy Impact Assessment

for

FOREST SERVICE APPLICATION CLOUD ENVIRONMENT (FS ACE)

Policy, E-Government and Fair Information Practices

Version: 1.11 (CY23 ATO / Review and Update)

Date: DECEMBER 15, 2022

Prepared for: USDA NRE FOREST SERVICE

USDA
United States Department of Agriculture

Contact Point

Zahid Chaudhry

System Owner

USDA NRE Forest Service

(503) 808-2440

Reviewing Official

Cynthia Ebersohn

Privacy Officer

USDA NRE Forest Service

386-301-4060

Abstract

The Forest Service Application Cloud Environment (FS ACE) is a general support system (GSS) that provides data center services for the United States Forest Service via a cloud hosting agreement with the United States Department of Agriculture (USDA), Digital Infrastructure Services Center (DISC).

Overview

The Forest Service (FS) Application Cloud Environment (FS ACE) is a General Support System (GSS) that resides at the US Department of Agriculture (USDA) Digital Infrastructure Services Center (DISC). FS ACE provides hosting services to six (6) Forest Service (FS) Resource Information Management (RIM) areas and their applications and all FS Regions part of the FS Virtual Data Center (VDC).

FS ACE provides each RIM and Region with a customer area cloud called a Customer Virtual Private Cloud (VPC) which is a conceptual container for their IT resource portfolios. FS ACE offers common, shared services and applications that support the FS RIM and Region IT portfolios such as Application Development and Deployment, Application Hosting, Data Hosting, and Enterprise Services. FS ACE hosts hundreds of applications within the 6 RIMS and Regions.

FS ACE runs on hardware including servers and networks that are the responsibility of DISC Midrange Systems which provides Infrastructure as a Service (IaaS) and is held under a Service Level Agreement (SLA). FS ACE does not include any hardware. DISC provides and maintains the virtual hosts and operating systems that are offered as a part of the services the FS contracts with DISC (in FS ACE this is Windows Enterprise Server and RedHat Enterprise Linux). The subsystems and software components that run on these servers are withing the accreditation boundary of FS ACE GSS unless they are included within the FISMA-boundary of another system/application.

FS ACE security model for each VPC establishes logical boundaries for three resource enclaves, DMZ, Internal Production, and Work Area. The DMZ is used to host applications that require access from non-FS networks, Internal Production enclave is used to host applications accessible from FS Networks, and Work Area is used to host development and test environments. Public facing applications are isolated to DMZ enclaves and public users will be authenticated by using the USDA eAuthentication (eAuth) system. A subset of FS ACE web applications is public facing and do not require authentication. Internal facing applications may only be accessed from FS Intranet and authenticated using the USDA eAuth system.

The users of FS ACE hosted applications are authenticated by FS ACE proxy servers against the USDA Enterprise Active Directory (EAD) or eAuth services and may also be subsequently authenticated and authorized via DISC Enterprise Data Center (EDC) (FS Organizational Unit (OU)), or Oracle Internet Directory (OID). FS ACE priviledged users are issued within the DISC Enterprise Data Center (EDC) Domain.

FS ACE shares relationships/interconnections with other boundaries/systems that have information sensitivity below.

-FS ACE shares an interconnection with USDA Identity, Credential, and Access Management (ICAM) Shared Service (formally known as eAuthentication) which provides FS ACE applications (FSAPPS) with single sign on (SSO) capability, management of user credentials, and verification of identity and authorization. FSAPPS is the nickname for the FS Application Authentication portal. This FSAPPS-Auth-Service is comprised of a security gateway mechanism for application authentication of internal Forest Service Applications using eAuth. It implements a solution to comply with OMB 11-11 mandate and PIV enforcement for Forest Service users with eAuth. ICAM Shared Services maintains its own Privacy Impact Analysis (PIA).

-FS ACE shares an interconnection with Electronic Management of the National Environment Policy Act (eMNEPA) to provide eAuth to the Planning Appeals & Litigation System (PALS) hosted at FS ACE. eMNEPA maintains its own PTA and PIA.

-FS ACE shares an interconnection to Login.gov to provide SSO capability, multi-factor authentication, and verification of identity and authorization for non-federated users. Login.gov is a user-centric identity management platform for delivering government services through a centralized platform.

-FS ACE shares an interconnection with Pay.gov to process financial transactions for purchases made on the National Symbols Cache site also known as Symbols.gov via the Internet with a single sign-on (SSO) capability, multi-factor authentication, and verification of identity and authorization and authorization for non-federated users.

FS ACE applications that collect, process, generate or store Personally Identifiable Information (PII) are identified below under their Deputy Area for Hosting Charges.

FSXCFOX - Chief Financial Officer

-Albuquerque Service Center, Budget and Finance Tools (ASC B&F Tools) is a set of applications which are used by the ASC Budget & Finance group to manage workflow using SQL Server databases and applications. ASC B&F Tools include:
IBS Reports (using FSApps Portal)
Claims Reports (using FSApps Portal)
IBS Job code Report

FS-6500-214 Security form and workflow management
FS-6500-214 Admin Tools (Version 1.1.4)
The tools are used by ASC B&F and Financial Management Systems personnel to track and assist in their daily work by tracking the progress of various service requests such as tracking requests for access to various Forest Service, and USDA financial systems.

ASC B&F Tools has information on Non-USDA Federal Employees and USDA Partners, and name and address on individuals, personal identification numbers, miscellaneous identification numbers and Handwriting or an image of the signature. This application utilizes security controls of encryption, masking of PII, controlled access, and timeout for remote access. No PII is shared with any USDA or non-USDA system. ASC B&F Tools does collect personal identification numbers to obtain, access and maintain information necessary in financial records in databased stored at the National Finance Center (NFC).

-TeamMate+ Audit is an audit management system that allows the Forest Service to identify risk and create assessment reports, schedule projects, allocate resources, capture time and expenses, track audits and issues, and create and manage audits via an advanced electronic working papers database. It is used for ASC B&F Automated Business Processes.

TeamMate+ has information on contractors and name and address, personal identification number, financial data, and miscellaneous identification numbers on individuals. This application utilizes security controls of encryption and controlled access. No PII is shared with any USDA or non-USDA system. TeamMate+ Audit does collect personal identification numbers which falls under the ASC B&F Tools application.

FSXOPSX - Business Ops or Infrastructure

-Employment Outreach is an Integrated Human Resources Management (HRM) & Services Portal (iHASP) application available to all FS Employees to post and search for employment opportunities prior to vacancy announcements being posted on USA Jobs. Postings include opportunities for temporary and permanent positions, student employment, details and temporary promotions. Its function using e-Authentication provides a role-based web application front end via an IIS server to an Oracle backend database. The security boundary is completely inside FS firewall/intranet infrastructure. The application can be accessed using ICAM Shared Services for FS employees using ConnectHR, the public can access through a separate URL to view and respond to notices by data entry.

Employment Outreach has information on USDA Employees, Contractors, Non-USDA Federal Government employees, USDA Partners, and the general public. The following information on individuals includes name and address, personal identification numbers, employment history and other information (disability rating, personal email, education history, email, phone number, and performance information). This application utilizes security controls of encryption, controlled access, timeout for remote access and system audit logs. PII is shared with another USDA system, Enterprise Application Development, National Finance Center. No PII is shared with any Non-USDA system. Employment Outreach may collect personal identification numbers by inadvertently providing social security number.

-Position Description (PD) Library is a component of HRM's iHASP system that is a searchable repository of Agency Standard Position Descriptions maintained by HRM classification specialists, as well as non-standard PDs maintained by the HR Service Teams (HRSTs). This application uses eAuth that provides role based application frontend via an IIS server to Oracle backend database. Security boundary is entirely within firewall/intranet infrastructure.

PD Library has information on USDA Employees and name and address on individuals. This application utilizes security controls of encryption, controlled access, and timeout for remote access. No PII is shared with any USDA or non-USDA system. PD Library does not collect personal identification numbers.

-Telework/Remote Work Agreement – This Enterprise solution will take the place of the legacy PDF form used to document the agreement between the employee and supervisor. The application is for requesting, initiating, approving, and modifying telework and remote work agreements. The application will impact employees and supervisors across the agency by providing an easy to navigate, accessible, robust application for telework agreements.

Telework/Remote Work Agreement has information on USDA Employees and name and address on individuals. This application utilizes security controls of encryption, controlled access, timeout for remote access and system audit logs. PII is shared with another USDA system, USDA National Finance Center, PAYPERS (Pay and Personnel) system for Employee and Position information. The system shares PII with Non-USDA Systems, Paycheck 8 (SaaS), for obtaining supervisors' managed employees
(GDC Integration, Inc.) and ConnectHR (SaaS), for obtaining authorized user information
(GDC Integration, Inc.). Telework/Remote Work Agreement does not collect personal identification numbers.

FSXNFSX - National Forest System

-Planning, Appeals, and Litigation System (PALS) is an application supporting the NEPA practitioner communities. PALS tracks planning projects, NEPA decisions, and appeals and litigation of those decisions. PALS uses eMNEPA's document management capabilities to store and publish project related publicly available appeal response documents to the public WWW. Users authenticate to applications hosted within AWS GovCloud by first authenticating to PALS hosted at FS ACE, which implements USDA eAuth. The single sign on capabilities between PALS and other eMNEPA applications are custom built, requiring USDA eAuth for authentication and authorization.

PALS has information on USDA Employees and Litigant/Appellant information (public information available from court documentation). The following information on individuals includes name and address. No PII is shared with any USDA or non-USDA system. PALS does not collect personal identification numbers. PALS is covered under the eMNEPA PTA.

-VSReports is a repository for reporting volunteer, community, and national service work program accomplishments. It is for internal FS users who report projects and work accomplished with partners and individuals, participant demographics, related expenditures, and other data. VSReports is hosted on the FS intranet only (accessible to FS users only) and is the companion to the Partner Portal (Volunteers and Service Portal aka VSPortal) who share the same database. VSPortal is the external facing (DMZ) application that will be used by partner organizations to perform data entry related to Volunteers and Service work performed for the Volunteer and Service Group. The Partner Portal enhancement improves the integrity of data collection and reporting in support of legislative authorities and workforce development priorities. Information reported via this system informs leadership decision making and is captured in annual Congressional budget reports and requests. Internal and external users are required to use eAuth to access the system.

VSReports/Partner Portal has information on others who have a specific degree of specific interest (Public Land Corps and others engaged in activities on FS units who are eligible for special hiring authorities and projects conducted by groups in partnership and individuals codified by a formal agreement instrument via partner organizations and their agreement with Forest Service). The following information on individuals includes name and address, date and place of birth, and other (ethnicity, race, education, gender). This application utilizes security controls of encryption, timeout for remote access and system audit logs. No PII is shared with any USDA or non-USDA system. VSReports and Partner Portal does not collect personal identification numbers.

FSXSNPF - State and Private Forestry

-Symbols.gov - The National Symbols program develops and distributes educational and promotional materials about conservation and wildfire prevention using Woodsy Owl, Smokey Bear and the Junior Ranger programs. Smokey Bear and Woodsy Owl are icons that represent national public service advertising campaigns recognized by two acts of Congress. Symbols provides ecommerce capability of FS merchandise to the general public.

Symbols has information on the general public and name and address on individuals. This application utilizes security controls of encryption, controlled access, timeout for remote access and system audit logs. PII is not shared with other USDA system. The system shares PII with Non-USDA Systems such as shipping companies that FS utilizes (i.e. FedEx, UPS, USPS). Symbols.gov does not collect personal identification numbers.

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?

The FS ACE GSS resources may process sensitive information of many types, including PII that relates to USDA & FS employees, contractors, Non-USDA Federal Government Employees, USDA Partner, the general public, vendors and others such as litigant/appellant public information, and participant information for Public Land Corps and others engaged in activities on FS units who are eligible for special hiring authorities and projects conducted by groups in partnership and individuals codified by a formal agreement instrument.

Depending on the application which is processing PII, the following PII types may include: Name, Place and Date of Birth, Street Address or Email, Personal Identification Number (social security number, tax identification number, passport number, driver’s license number or an otherwise unique identification number), Financial data (credit card numbers, bank account numbers),, Employment history, Miscellaneous Identification Numbers (agency assigned number, case number, accounts, permits), Handwriting or an image of the signature and other information that may be seen as personal characteristics such as disability rating, education history, phone number, performance information, ethnicity, race, gender.

1.2 Source

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

Information processed by the FS ACE GSS is obtained by FS staff in connection with the Agency’s conservation functions and other activities. This may include information that is submitted by individuals or shared between FS applications.

1.3 Justification

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

Information in the FS ACE GSS is collected, used, disseminated, and maintained for the Agency to perform its conservation functions and other activities. FS-approved personnel may collect and use the information to: remit payments to individuals, businesses and organizations; collect payments; and administer agency financial processes.

1.4 Collection

How is the information collected?

The FS ACE GSS collects and processes information from the applications within the FS ACE boundary. This information may be collected via fax, email, form, telephone or web site.

1.5 Validation

How will the information be checked for accuracy?

Information in the FS ACE GSS that is used by the Forest Service, as part of its conservation, and any other activities will be reviewed for accuracy as required by the particular activity or business unit. For example, staff preparing a remittance will check the accuracy of the individual's information against the source (fax, email, etc.) and an auditor will review the entry to ensure its accuracy prior to approving the release of funds.

1.6 Authority

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

The Forest Service operates under several US Code titles and chapters including those that regulate federal agency administration and those pertaining to the conservation and management of the nation's renewable resources. As a general support system for Forest Service operations, FS ACE may process data authorized within these laws and regulations.

- The Financial Services Modernization Act (for financial applications)
- The Health Insurance Portability and Accountability Act (for health-related applications)
- The Electronic Communications Privacy Act (for any application transmitting information electronically)
- The Data Privacy Act of 1974

- FIPS 199 (Standards for Security Categorization)For FS ACE, authorities for general collection of information come from by 31 U.S.C. 3512, Executive Agency Accounting Systems Act of September 12, 1950, and 16 U.S. Code § 551 - Protection of national forests; rules and regulations.

Federal requirements for the collection of information, also see: 5 U.S.C. Chapter 552 (Freedom of Information Act), 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071 (Concealment, removal, or mutilation of govt records)

U.S.C. 3101 et seq. (financial), 44 U.S.C. 3506 (Federal Agency Responsibilities), 36 CFR Chapter 12, Subchapter B (Records Management), 36 CFR Part 1234 (Handling Deviations From NARA's Facility Standards), 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 Schedules.

1.7 Risk Mitigation

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

The following privacy risks were considered during the development of the FS ACE GSS:

Malicious Code: To address these risks, the FS employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure.

Hackers: To address this risk, the FS implements a defense-in-depth strategy in the FS ACE GSS by applying mutually supporting security controls to the networks, hosts, and applications.

Unauthorized Access to Data (Logical and Physical Access): To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to network user IDs upon creation. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the FS ACE GSS is controlled, logged, and monitored by DISC.

Misconfigured information asset: To address this risk, the FS has deployed a strict configuration management program to approve and document all configuration changes made to FS ACE GSS IT assets.

Information loss through IT asset decommissioning: To address this risk, all IT asset hard drives are sanitized before reuse or destroyed.

Mishandling of privacy data: FS employees must complete privacy training prior to receiving a user account that addresses the identification and proper handling of privacy data.

Incident response: In the event information technology resources are lost, stolen or compromised the FS has a robust incident response capability for identifying the incident, minimizing the damage, restoring capabilities and reporting the impact.

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.

> Business applications that are supported by the FS ACE GSS use the information to support Forest Service conservation functions and other activities to include: managing contracts, remitting payments, collecting payments, managing vendors, and administrative functions related to human resources, security, financial management, and resource management.

2.2 Analysis and Production

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

> FS ACE use reports, database queries, and application interfaces that are used to analyze the data collected by the business activity.
>
> The CI/CD Pipeline is being configured to allow for automated deployments utilizing the existing applications of GitHub, Jenkins and Puppet. The CI/CD Pipeline provide deployment automation leveraging GitHub and Jenkins in Azure Commercial Cloud to facility deployments and code updates to Artifactory and the Docker Trusted Registry (DTR) in the VDC. Orchestration for Docker is also accomplished through Puppet in the VDC.

2.3 Commercial/Public Use

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

> FS ACE does not support applications using commercial or publicly available privacy 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.

Not Applicable. None of the data comes from commercially or publicly available sources. Physical access to the FS ACE GSS is controlled, logged, and monitored by DISC.

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?

FS ACE retains system maintenance, operations and security information for at least 5 years in accordance with approved NARA record schedules: GRS 3.1 and 3.2.

3.2 Approval

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

Yes

3.3 Risk Mitigation

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

Unauthorized Access to Data (Logical and Physical Access): To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to network user IDs upon creation. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the FS ACE GSS is controlled, logged, and monitored by DISC.

Mishandling of privacy data: Forest Service employees must complete privacy training prior to receiving a user account that addresses the identification and proper handling of privacy data. Users also receive annual records management training.

Information loss through IT asset decommissioning: To address this risk, all IT asset storage media are sanitized before reuse or destroyed.

Retaining information too long: As part of the Forest Service certification and accreditation process, each application must certify that it retains records in accordance with Federal laws, regulations and policies. This includes the application’s approved record schedule and applicable System of Record Notices (SORN).

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?

N/A

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

N/A

4.3 Risk Mitigation

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

N/A

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?

FS ACE shares information with GSA and U.S. Treasury.

GSA – Login.gov: The Forest Service may send to GSA/TTS the email address, SMS phone number, and other unique identifiers for storing (applicable user group) in standalone login.gov identity management platform. Users will be authenticated and proofed at the level required by the Forest Service for accessing specific services and records.

U.S. Treasury – Pay.gov: The data that traverses this connection contains federal financial information as well as Privacy Act data and is classified Sensitive but Unclassified (SBU). The purpose of this connection is to collect the financial data of the customers purchasing merchandise through Forest Service e-commerce websites.

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.

Yes, it is covered by the FS ACE SORN.
https://www.govinfo.gov/content/pkg/FR-2021-07-06/pdf/2021-14278.pdf
#FS-63, published in the Federal Register 7/6/2021

5.3 Delivery and Security Measures

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

GSA – Login.gov: The information is shared via an API that is encrypted via TLS. The connection is limited to the cloud.gov egress IP addresses.

U.S. Treasury – Pay.gov: SNA and TCP/IP traffic between Fiscal Service TWAI Applications and BP are over a VPN Tunnel using encryption methods described in the SSP.

5.4 Risk Mitigation

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

Malicious Code: To address these risks, the Forest Service employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure.

Hackers: To address this risk, the Forest Service implements a defense-in-depth strategy in the FS ACE GSS by applying mutually supporting security controls to the networks, hosts, and applications.

Unauthorized Access to Data (Logical and Physical Access): To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to network user IDs upon creation. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the FS ACE GSS is controlled, logged, and monitored by DISC.

Misconfigured information asset: To address this risk, the Forest Service has deployed a strict configuration management program to approve and document all configuration changes made to FS ACE GSS IT assets.

Incident response: In the event information technology resources are lost, stolen or compromised the Forest Service has a robust incident response capability for identifying the incident, minimizing the damage, restoring capabilities and reporting the impact.

Mishandling of privacy data: Forest Service employees must complete privacy training prior to receiving a user account that addresses the identification and proper handling of privacy data.

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.

> Yes, USDA/FS-63 Application Cloud Environment (FS ACE), published in the Federal Register 7/6/2021:
>
> https://www.govinfo.gov/content/pkg/FR-2021-07-06/pdf/2021-14278.pdf

6.2 Individual Notification

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

> For information that is collected pursuant to a request from the Forest Service, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). The Forest Service also provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and this PIA.

6.3 Right to Decline

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

> Yes, individuals who send inquiries to the Forest Service, and provide information about themselves voluntarily, and could choose to decline to provide such 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?

Yes, individuals who send inquiries to the Forest Service, and provide information about themselves voluntarily, and could choose to decline to provide such 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.

For information that is collected pursuant to a request from the Forest Service, notice is generally provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). The Forest Service also provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and this PIA. In the event an individual believes a Forest Service system has inappropriately collected their personal information, they may contact the Forest Service Privacy Office and review FS Privacy Policy by visiting the USDA Privacy Policy website.

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?

Individuals seeking access to records contained in this system of records, or seeking to contest content, may submit a request in writing to the Forest Service FOIA/Privacy Act Officer. If an individual believes more than one Department component maintains Privacy Act records concerning him or her, the individual may submit the request to the Departmental FOIA Officer, 1400 Independence Avenue SW, South Building Room 4104, Washington, DC 20250-0706, or email the USDA FOIA at USDAFOIA@ocio.usda.gov.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

7.3 Notification

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

Privacy Impact Assessment Forest Service Application Cloud Environment (FS ACE) on the Department Privacy Impact Assessment website.

Forest Service-specific System of Records Notices are published on the Forest Service SORN website.

7.4 Redress Alternatives

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

7.5 Risk Mitigation

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

For information that is collected pursuant to a request from the FS, notice is generally provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). The FS also provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and this PIA.

In the event an individual is uncertain how to perform this function, they may contact the FS Privacy Office and review FS Privacy Policy by visiting the USDA Privacy Policy website.

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?

All Forest Service positions are assigned a risk designation and associated personnel screening criteria. All potential Forest Service network users are subject to background investigations and suitability reviews per OMB guidance. In addition, before any new employee, contractor, or volunteer can access the FS ACE, they must first complete the Forest Service's Privacy and Security Awareness training and a network user request form that is validated by a supervisor or government sponsor.

Furthermore, there are additional procedures to address access restrictions for access to business applications and to specify the appropriate access privileges. Network and application access are based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access are based on least-privilege and need-to-know security models.

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 Federal Agency employees and FS contractors are required to take annual security awareness and privacy training in accordance with Federal requirements.

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, FS ACE has an ATO that expires January 25, 2024

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, user identification and authentication, the use of network and application access controls, the auditing of significant changes to systems or data, system and data backups, intrusion detection capabilities, anti-malware software, and restricted physical access to the servers and storage media.

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?

The following privacy risks were considered during the development of the FS ACE GSS:

Malicious Code: To address these risks, the Forest Service employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure.

Hackers: To address this risk, the Forest Service implements a defense-in-depth strategy in the FS ACE GSS by applying mutually supporting security controls to the networks, hosts, and applications.

Unauthorized Access to Data (Logical and Physical Access): To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to network user IDs upon creation. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the FS ACE GSS is controlled, logged, and monitored by DISC.

Misconfigured information asset: To address this risk, the Forest Service has deployed a strict configuration management program to approve and document all configuration changes made to FS ACE GSS IT assets.

Incident response: In the event information technology resources are lost, stolen or compromised the Forest Service has a robust incident response capability for identifying the incident, minimizing the damage, restoring capabilities and reporting the impact.

Mishandling of privacy data: Forest Service employees must complete privacy training prior to receiving a user account that addresses the identification and proper handling of privacy data.

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?

FS ACE is a GSS with a MODERATE security impact that resides on USDA DISC. FS ACE provides hosting services to six (6) Forest Service (FS) Resource Information Management (RIM) areas and their applications and all FS Regions part of the FS Virtual Data Center.

DISC provides and maintains the virtual hosts and operating systems in FS ACE (Windows Enterprise Server and RedHat Enterprise Linux). The subsystems and software components that run on these servers are withing the accreditation boundary of FS ACE GSS unless they are included within the FISMA-boundary of another system/application.

9.2 Privacy Concerns

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

FS ACE uses cloud-based technologies to promote cost savings and the efficient use of government IT resources. Cloud-based technologies may present several privacy concerns including a decreased awareness of the cloud environment’s security status and capabilities, the availability of privacy information to external contractors and the responsible agency’s loss of physical control of the data. FS ACE has mitigated these concerns by contracting cloud services with another USDA function, DISC. This organization and its supporting infrastructure have completed the Federal certification and accreditation process. In addition, by utilizing DISC, the Forest Service has retained control of privacy data within the Department and limited physical access to USDA vetted employees and contractors.

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?

N/A

10.3 PII Availability

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

N/A

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?

N/A

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?

N/A

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?

N/A

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?

N/A

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?

N/A

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)?

N/A

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?

N/A

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?

N/A

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.

N/A

Responsible Official

ZAHID CHAUDHRY Digitally signed by ZAHID CHAUDHRY Date: 2023.05.11 16:19:31 -04'00'

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: 2023.05.30 08:47:03 -05'00'

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

BENJAMIN MOREAU Digitally signed by BENJAMIN MOREAU Date: 2023.06.10 21:53:21 -04'00'

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