Privacy Impact Assessment

for

Forest Service End User Computing Environment (FS-EUCE)

Policy, E-Government and Fair Information Practices

Version: 1.7

Date: Mar 3, 2020

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

Contact Point

Kevin R. Crupper

Information System Security Officer

USDA NRE Forest Service

505-379-8154

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

This assessment pertains to the Forest Service End User Computing Environment (FS EUCE) General Support System. The EUCE is comprised of end user devices such as desktops, laptops, and tablet computers, and smart phones. The EUCE is a general support system that has the ability to interface with multiple other systems that collect and retain PII and therefore a PIA has been prepared.

Overview

The FS EUCE is managed by the USDA Forest Service. The EUCE provides end user resources to support the daily operations of the Forest Services. The EUCE is widely dispersed around the United States within Regional, Forest, District, and Research Station offices.

The EUCE is comprised of end user devices such as desktop, laptop, and tablet computers and smart phones. These devices provide the primary means for all FS employees to connect to and interact with multiple Agency and Departmental IT services as well as the World Wide Web.

EUCE recognizes that employees across the Forest Service who are authorized to work with PII will sometimes store PII on their computers (endpoints) to accomplish their work, and that PII will sometimes be present on Forest Service endpoints and therefore EUCE. For example, PII data related to law enforcement systems or human resource management systems can be temporarily stored on a desktop or laptop, worked with by employees, and then loaded back onto the primary system. EUCE cannot actively monitor the movement of PII data, EUCE cannot with any certainty identify what PII is on EUCE at any given moment in time. Additionally, the PII that is on EUCE would be continuously changing, so even if EUCE could take a snapshot of PII content, it would no longer be accurate a short time after it was assessed.

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 EUCE is not intended to be used for data storage and dissemination however natural resource information may be stored temporarily while data is collected and processed in the field. Handling of PII is discussed in the mandatory Forest Service Rules of Behavior training.

The EUCE GSS connects to multiple other systems for a wide variety of purposes. Some of these systems may contain PII. EUCE devices could typically be used to make connections to systems containing PII and then function as data entry conduits or means to view PII.

The other connected systems include, but are not limited to:

Connect HR, GovTrip, Leimars, NFC, Oracle Content Database, Citrix and ITSDS

PII may include:

Name (mother's maiden name, maiden name of the individual, nickname, or alias).

Date and/or place of birth.

Address Information (street or email address).

Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number)

Financial data (credit card numbers, bank account numbers, etc.).

Health data (including height, weight, blood pressure, etc.).

Biometric data (fingerprints, iris scans, voice signature, facial geometry, DNA, etc.).

Criminal history.

Employment history.

Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, etc.).

Photographic image/identifying characteristics.

Handwriting or an image of the signature.

Other information that may be seen as personal (personal characteristics, etc).

1.2 Source

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

Sources of data in the EUCE can be entered by FS employees, obtained from downloads, or be sourced by a wide variety of sensors and instruments used in the field.

1.3 Justification

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

The EUCE is primarily used to collect and process natural resource information which is then transmitted to other systems for permanent storage and dissemination.

1.4 Collection

How is the information collected?

Natural resource information may be collected by a variety of means such as end user manual entry, downloads from other systems including the World Wide Web, connections to various instruments or sensors such as a traffic counter or a global positioning system (GPS) receiver, or other devices like digital cameras.

EUCE devices may also interface with other systems and act as conduits for data collection such as when connected to another system or server by way of a web interface and keystrokes are transmitted to the server to complete a form. These other systems named above may contain PII.

1.5 Validation

How will the information be checked for accuracy?

Given the nature of the EUCE and its diverse use it is expected that other systems have their own means and procedures for assurance of information accuracy.

1.6 Authority

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

F S Policy 6640.42i – Employees

It is the responsibility of the employee to: Understand there is no expectation of privacy with government provided telecommunications equipment. Records and usage of any equipment can be requested and examined by management at any time, without prior notification of the employee.

1.7 Risk Mitigation

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

Devices within the EUCE that interface with other systems that may contain PII must be authenticated to by entering a unique username and password that has been assigned to each end user by the Chief Information Office (CIO) Application Hosting Line of Service (AHLOS). End user passwords must be changed at regular intervals and meet the minimum password requirements of the Agency. Once a user is authenticated, EUCE relies on the controls of the system to which it interfaces with for further privacy risk mitigation. User access to EUCE is still controlled with a logon process.

The EUCE is a means to interface with multiple other systems that may contain PII. It is impracticable to describe analytic tools and data types for each system the EUCE may interface with.

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.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FSIS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: USDA or any component thereof; any employee of FSIS in his/her official capacity; any employee of FSIS in his/her individual capacity where DOJ or FSIS has agreed to represent the employee; or the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and FSIS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which FSIS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when: FSIS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely

upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FSIS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FSIS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of FSIS or is necessary to demonstrate the accountability of FSIS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

To appropriate agencies, entities, and persons when: FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

2.2 Analysis and Production

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

The EUCE is a means to interface with multiple and various other systems that may contain PII. It is impracticable to describe analytic tools and data types for each system the EUCE may interface with.

2.3 Commercial/Public Use

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

It is likely that the system will interface with publicly available data, however it does not use commercial information.

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.

It is expected that systems the EUCE may interface with have the proper controls in place to ensure that information is handled in accordance with the above described uses.

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?

Many differing types of records will be a part of this General Support System. It is expected that systems the EUCE may interface with have defined retention periods. EUCE does not retain PII.

3.2 Approval

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

It is expected that systems the EUCE may interface with have approved retention periods.

3.3 Risk Mitigation

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

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have addressed risk and mitigations concerning data retentions.

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?

The EUCE does not directly share information. EUCE is a means to interface with multiple other systems that may contain PII. The environment allows data sharing between end-user devices and other systems, but EUCE as a whole is not a system that shares data. It is expected that systems the EUCE may interface with have identified their information sharing policies. EUCE connects to multiple other systems, such as: ConnectHR, LEIMARS, GovTrip, Aglearn, NFC, ITSDS and eCollections.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

The EUCE does not directly share information.

4.3 Risk Mitigation

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

It is expected that systems the EUCE may interface with have addressed risk and mitigations associated with information sharing and disclosure.

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.

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. 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.

5.3 Delivery and Security Measures

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

Not Applicable.

5.4 Risk Mitigation

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

The EUCE is a means to interface with multiple other systems that may contain PII. The EUCE does not share data externally.

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 and if so, please provide SORN name and URL?

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

No

6.2 Individual Notification

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

It is expected that systems the EUCE may interface with have notice policies.

6.3 Right to Decline

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

It is expected that systems the EUCE may interface with have notice policies.

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?

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have addressed risk and mitigations associated with notice to individuals.

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.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

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?

All FS personnel can log into and gain access to the various EUCE systems to view their own personal information contained in other systems to which it connects and the need to know. At any point, these persons can contact the FS to inquire about the information contained in the connected system. Specifically, these persons can contact the Freedom of Information Act Office:

USDA FS, FOIA Service Center
1400 Independence Avenue SW
Mail Stop 1143
Washington, DC 20250-1143

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

There is no set/defined communication procedure regarding information correction, nor is a formal process needed. FS personnel can edit erroneous information in systems connected to the EUCE. As for requesting members of the public who would like to have their information corrected, the FS program or project managers that have been alerted as to the error(s) can complete the needed correction.

7.3 Notification

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

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have defined policies concerning individual notification and correction of information.

7.4 Redress Alternatives

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

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have defined polices for redress.

7.5 Risk Mitigation

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

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have addressed risk and mitigations associated with redress.

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?

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have documented user access policy. The EUCE does have documented procedures in place regarding end user access and is described further in section 1.7.

8.2 Contractor Access

Will Department contractors have access to the system?

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have policy regarding contractor access. Contractors are allowed access to the EUCE

8.3 Privacy Training

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

Security Awareness and privacy training is provided by the Aglearn system for end users of the EUCE. Each user of the EUCE must undergo the Department's Security Awareness training prior to being granted access to the system. Users must also complete Security Awareness refresher training yearly in order to retain access to the system. The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with provide relevant training specific to that system.

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).

The EUCE is currently undergoing a new Security Authorization due to significant changes and transformation of the system formerly known as FSCB Legacy to the EUCE. The EUCE is a means to interface with multiple other systems that may contain PII. It is unknown if all systems the EUCE may interface with have completed Certification and Accreditation.

8.5 Audit and Technical Safeguards

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

The EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have auditing measures and technical safeguards to prevent data misuse. In addition, the EUCE does require authentication and laptop devices that may interface with systems containing PII are encrypted.

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 EUCE is a means to interface with multiple other systems that may contain PII. It is expected that systems the EUCE may interface with have identified any privacy risks and addressed mitigations for those risks. Additionally, the EUCE does require authentication and laptop devices that may interface with systems containing PII are encrypted.

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?

The Forest Service End User Computing Environment (EUCE) is a General Support System. It is widely dispersed around the United States in Regional, Forest, District, and Research Station offices. Devices within the EUCE are often the primary access tool to IT products and services provided by the Agency.

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

OMAR THOMPSON
Digitally signed by OMAR THOMPSON
Date: 2020.04.30 09:26:39 -05'00'

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

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2020.04.29 18:06:58 -05'00'

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

LAURA HILL
Digitally signed by LAURA HILL
Date: 2020.05.04 08:11:02 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture