



U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement, PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available [here](#).



Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:

Joint Azure Resource Virtualized Information System (JARVIS)

Natural Resources and Environment (NRE) Forest Service (FS)

Date PIA submitted for review:

9/10/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Cynthia Lee Ebersohn	Cynthia.ebersohn@usda.gov	386-301-4060
Information System Security Officer	Tasha Middleton	Tasha.middleton@usda.gov	816-708-8310
System Owner	Zahid Chaudhry	Zahid.chaudhry@usda.gov	503-808-2440

Abstract

The Natural Resources and Environment Forest Service Joint Azure Resource Virtualized Information System (NRE FS JARVIS) is a General Support System (GSS) operated and managed by the US Forest Service (FS) Office of the Chief Information Officer (CIO). NRE FS JARVIS is an integrated cloud-based solution provided by Microsoft Azure Government Software as a Service (SaaS), FedRAMP accredited cloud resources that allows for secure cloud storage, sharing and collaboration. A Privacy Threshold Analysis (PTA) was performed, indicating that a Privacy Impact Analysis (PIA) must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

Microsoft Azure SaaS provides FS with the capabilities needed to collect data, investigations, and Freedom of Information Act (FOIA) requests including cloud-based collections, processing, culling, and review. All data is subject to the organization policies in place to govern this data, to include privacy and organization-level security. Microsoft Azure SaaS is responsible for the overall delivery of the application from the physical to transport layers. NRE FS JARVIS is responsible for controls related to the usage of the Microsoft Azure SaaS service including the management of user access, permissions, and application security configurations. NRE FS JARVIS is responsible for session, presentation, and application layer management as outlined within the NRE FS JARVIS SSP and Control Implementation tab of the Cyber Security Assessment and Management (CSAM) entry. NRE FS JARVIS relies on most technical controls from Microsoft Azure Government Software as a Service (SaaS), FedRAMP accredited cloud resources.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

This system is regulated by privacy laws, regulations, and government requirements, in addition to the Privacy Act (5 U.S.C. §101); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501):

Job Corp legal authority to collect information comes from 20 CFR Part 686 – the Job Corps Under Title I of the Workforce Innovation and Opportunity Act

Symbols.gov and Symbols Royalty- Woodsy Owl-Smokey Bear Act of 1974 (Public Law 93-318): This Act established Woodsy Owl as a "symbol for a public service campaign to promote wise use of the environment and programs which foster maintenance and improvement of environmental quality." The Act gave responsibility for Woodsy Owl to the Forest Service.

The 1990 Farm Bill, Forest Stewardship Act of 1990 (16 U.S.C. 2101: Under the Urban and Community Forestry Assistance Program, the Secretary, in cooperation with State Foresters, State Extension Directors and interested members of the public, including nonprofit private organizations, shall implement a program of education for urban and community forest resources. As part of the Forest Stewardship

Program, the Secretary is authorized to provide education and related assistance to State Foresters, including financial assistance to other State and local entities and land grant universities to deliver information to nonindustrial private landowners.

The National Environmental Education Act of 1990 (20 U.S.C. 5501: This Act restated the goal of the 1970 Environmental Education Act and stated, "Federal natural resource agencies such as the United States Forest Service have a wide range of environmental expertise and a long history of cooperation with educational institutions and technology transfer that can assist in furthering the purposes of the Act."

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

Yes, 10/4/2024.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

Job Corp- [DOL/GOVT-2](#) (DOL is responsible for this SORN)

Symbols.gov- USDA/FS-19 is currently in the process of being updated.

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2.0 Characterization of the Information

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

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers			
<input checked="" type="checkbox"/>	Social Security number	<input type="checkbox"/>	Truncated or Partial Social Security number

<input type="checkbox"/>	Driver's License Number	<input type="checkbox"/>	License Plate Number		
<input type="checkbox"/>	Registration Number	<input checked="" type="checkbox"/>	File/Case ID Number		
<input type="checkbox"/>	Student ID Number	<input type="checkbox"/>	Federal Student Aid Number		
<input type="checkbox"/>	Passport number	<input type="checkbox"/>	Alien Registration Number		
<input type="checkbox"/>	DOD ID Number	<input type="checkbox"/>	DOD Benefits Number		
<input checked="" type="checkbox"/>	Employee Identification Number	<input type="checkbox"/>	Professional License Number		
<input checked="" type="checkbox"/>	Taxpayer Identification Number	<input checked="" type="checkbox"/>	Business Taxpayer Identification Number (sole proprietor)		
<input type="checkbox"/>	Credit/Debit Card Number	<input type="checkbox"/>	Business Credit Card Number (sole proprietor)		
<input type="checkbox"/>	Vehicle Identification Number	<input type="checkbox"/>	Business Vehicle Identification Number (sole proprietor)		
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Business Bank Account Number (sole proprietor)		
<input type="checkbox"/>	Personal Device Identifiers or Serial Numbers	<input type="checkbox"/>	Business device identifiers or serial numbers (sole proprietor)		
<input type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Business Mobile Number (sole proprietor)		
<input type="checkbox"/>	Health Plan Beneficiary Number				
Biographical Information					
<input checked="" type="checkbox"/>	Name (including nicknames)	<input checked="" type="checkbox"/>	Sex	<input checked="" type="checkbox"/>	Business Mailing Address (sole proprietor)
<input type="checkbox"/>	Date of Birth (MM/DD/YY)	<input checked="" type="checkbox"/>	Ethnicity	<input type="checkbox"/>	Business Phone or Fax Number (sole proprietor)
<input type="checkbox"/>	Country of Birth	<input type="checkbox"/>	City or County of Birth	<input type="checkbox"/>	Group/Organization Membership
<input type="checkbox"/>	Citizenship	<input type="checkbox"/>	Immigration Status	<input type="checkbox"/>	Religion/Religious Preference
<input checked="" type="checkbox"/>	Home Address	<input checked="" type="checkbox"/>	Zip Code	<input checked="" type="checkbox"/>	Home Phone or Fax Number
<input type="checkbox"/>	Spouse Information	<input type="checkbox"/>		<input type="checkbox"/>	Children Information
<input type="checkbox"/>	Marital Status	<input type="checkbox"/>	Military Service Information	<input type="checkbox"/>	Mother's Maiden Name
<input checked="" type="checkbox"/>	Race	<input type="checkbox"/>	Nationality	<input type="checkbox"/>	Global Positioning System (GPS)/Location Data
<input checked="" type="checkbox"/>	Personal e-mail address	<input checked="" type="checkbox"/>	Business e-mail address	<input type="checkbox"/>	Personal Financial Information (including loan information)
<input type="checkbox"/>	Employment Information	<input type="checkbox"/>	Alias (username/screenname)	<input type="checkbox"/>	Business Financial Information (including loan information)
<input type="checkbox"/>	Education Information	<input type="checkbox"/>	Resume or curriculum vitae	<input type="checkbox"/>	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
<input type="checkbox"/>	Fingerprints	<input type="checkbox"/>	Palm prints	<input type="checkbox"/>	Vascular scans
<input type="checkbox"/>	Retina/Iris Scans	<input type="checkbox"/>	Dental Profile	<input type="checkbox"/>	Scars, marks, tattoos
<input type="checkbox"/>	Hair Color	<input type="checkbox"/>	Eye Color	<input type="checkbox"/>	Height
<input type="checkbox"/>	Video recording	<input type="checkbox"/>	Photos	<input type="checkbox"/>	Voice/ Audio Recording
<input type="checkbox"/>	DNA Sample or Profile	<input type="checkbox"/>	Signatures	<input type="checkbox"/>	Weight
Medical/Emergency Information					
<input type="checkbox"/>	Medical/Health Information	<input type="checkbox"/>	Mental Health Information	<input type="checkbox"/>	Disability Information

<input type="checkbox"/>	Workers' Compensation Information	<input type="checkbox"/>	Patient ID Number	<input type="checkbox"/>	Emergency Contact Information
Device Information					
<input type="checkbox"/>	Device settings or preferences (e.g., security level, sharing options, ringtones)	<input checked="" type="checkbox"/>	Cell tower records (e.g., logs, user location, time, etc.)	<input type="checkbox"/>	Network communications data
Specific Information/File Types					
<input type="checkbox"/>	Personnel Files	<input type="checkbox"/>	Law Enforcement Information	<input type="checkbox"/>	Credit History Information
<input type="checkbox"/>	Health Information	<input type="checkbox"/>	Academic/Professional Background Information	<input type="checkbox"/>	Civil/Criminal History Information/Police Record
<input type="checkbox"/>	Case files	<input type="checkbox"/>	Security Clearance/Background Check	<input type="checkbox"/>	Taxpayer Information/Tax Return Information

2.2. What are the sources of information in the system/program?

Job Corps- collects the following information that may be considered Personally Identifiable Information (PII): first name, last name, middle initial, personal and work email addresses, gender, personal phone number, ethnicity, and race.

Symbols.gov- collects the following information that may be considered Personally Identifiable Information (PII): first name, last name, personal and/or work email addresses, work and home addresses, and work and/or personal phone number.

Symbols Royalty- collects the following information that may be considered Personally Identifiable Information (PII): first name, last name, personal and/or business email addresses, business and home addresses, business and/or personal phone number, social security number, Employee/Employer Identification Number, Taxpayer Identification Number, and Business Taxpayer Identification Number.

2.2.1. How is the information collected?

Job Corps- Data is manually retrieved from a Department of Labor (DOL) system and manually re-entered into the JARVIS system. There are no physical or logical connections between JARVIS and the DOL system.

Symbols.gov- Information is collected directly by the public on-line placing the order and by request an USDA Partner aiding the public in submitting an order over the phone.

Symbols Royalty – Information is collected by vendors completing web forms through the portal.



Privacy Impact Assessment

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No

2.4. How will the information be checked for accuracy? How often will it be checked?

Job Corp- Forest Service (FS) employees verify the accuracy of JARVIS data by reviewing it after entering it into the JARVIS system.

Symbols.gov- The PII information entered by customers is not checked for accuracy. All PII entered into the system is entered by the customers and it is their individual responsibility to ensure the accuracy of the information entered into the Symbols.gov application. Verify the email is an accurate email format and/or any phone numbers entered are in the standard 10-digit phone format.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

N/A- Third party websites and/or applications are not used for NRE FS JARVIS

2.5.1.1. What PII will be made available to the agency through the use of third-party websites?

N/A- Third party websites and/or applications are not used for NRE FS JARVIS.

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of Information.

Follow the format below:

Privacy Risk: The potential risk for characterization of the information is the collection of irrelevant or unnecessary information that is not needed for the purposes of hosted applications within the NRE FS JARVIS security boundary.

Mitigation: Hosted applications that collect PII within the security boundary of NRE FS JARVIS are reviewed as part of their onboarding into the system boundary and as part of change management and security and privacy impact analyses. Hosted applications are expected to provide justification and evidence that supports the purpose and/or purposes for why PII must be collected, used, disseminated, or maintained in the system/program.

Section 3.0 Uses of the Information



Privacy Impact Assessment

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

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Job Corp- The principal purpose of the data being collected is to document information about individuals participating in the Job Corps program, and generating metrics associated with the participation of all individuals.

Symbols.gov- The PII information entered into the application is utilized strictly for the purposes of conducting the financial transaction and shipping the items the individual selected to purchase.

Symbols Royalty- The PII and business identification information entered into the application is used strictly to verify the payment is associated to the specific vendor and license.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk: The potential risk is the unauthorized use of PII data.

Mitigation: Only authorized users can make queries in NRE FS JARVIS. Teams are alerted when anomalous activities indicating unusual and potentially harmful attempts to exploit the databases (SQL Injections).

Section 4.0 Notice

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

4.1. How does the project/program/system provide notice to individuals prior to collection?

Job Corp privacy and security statement is located on their website at: <https://www.jobcorps.gov/privacy>

Symbols.gov has adopted USDA Privacy Policy located at: <https://www.usda.gov/privacy-policy>

Symbols Royalty- Corporations or individuals interested in becoming an Official Smokey Bear Licensee to produce and market products using the Smokey Bear and/or Woodsy image and/or likeness must



Privacy Impact Assessment

submit their information to validate their business. Specified in the license and terms of royalty reporting and payments.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

Job Corp- N/A

Symbols.gov- No, www.symbols .gov is an e-commerce site. PII data is available to authorized government users to pull user reports in shipping out items the individuals ordered.

Symbols Royalty- No option

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: Individuals unaware of the collection of their data.

Mitigation: Individuals have the choice of whether to pay by e-commerce. If they choose to pay by e-commerce, they are voluntarily submitting any personal information that may be displayed to complete the order. Forest Service point-of-sale locations have notifications that prominently explain what information may be collected and how that information will be used.

Section 5.0 Data Retention

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

5.1. What information is retained and for how long?

Job Corp- 1830- Volunteers and Service Programs. The FSH 6209.11- Records Management Handbook. Information regarding Job Corp is retained for a minimum of three (3) years.

Symbols.gov- 1380- Information Collection. The FSH 6209.11- Records Management Handbook. Information is retained for a minimum of six (6) years.

Symbols Royalty- Information Collection is retained for the term of the license. Business Information is retained for a minimum of three (3) years.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes, NRE FS JARVIS worked with NARA to agree on retention times to comply with The Federal Records Act which says that agencies must be maintaining adequate and proper documentation of policies and transactions of the Federal Government.

Job Corp- "1830- Volunteers and Service Programs"



Privacy Impact Assessment

Symbols.gov- “1380- Information Collection”

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk: The potential risk is extensive data retention.

Mitigation: Data is retained in accordance with specified guidelines and is protected using access controls and encryption.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

N/A

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: The potential risk is unauthorized access to PII.

Mitigation: Existing access controls prevent unauthorized access and/or modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data to which they intend to have access. Check images are stored for further processing in NRE FS JARVIS cloud components. Data-in-transit and data-in-rest are securely transmitted and stored in NRE FS JARVIS cloud environment. Only a limited number of roles can have access to these check images on a need-to-know basis to resolve system issues for further processing and settlement activities. Roles are tested to ensure that they can only get to the data to which they intend to have access.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NRE FS JARVIS connects to the following:

Department of the Treasury’s Pay.gov System: Pay.gov is the system used by the Treasury to collect credit card payments for educational and promotional materials about conservation and wildfire



Privacy Impact Assessment

prevention using Woodsy Owl, Smokey Bear and the Junior Ranger programs. Symbols.gov uses information collected from Pay.gov to settle sales purchased through Symbols.gov.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: The potential risk is data breaches. External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Mitigation: The information is transmitted using the secure transmission protocols required by the Treasury for any agency connecting to their mandated financial partners (Federal Reserve Bank of Cleveland and Comerica Bank). This connection is limited to the egress Internet Protocol (IP) addresses as established by the US Forest Service and the US Treasury Interconnection Security Agreements (ISA). PII data on credit cards is transmitted to the Treasury-designated credit card processor (Worldpay), data transmission is encrypted using treasury mandated protocols immediately upon collection of PII data to Worldpay.

Section 7.0 Redress

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

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

Job Corp- The individuals do not have access to their information. The accuracy of the PII information contained within Job Corp is validated upon initial record creation in the DOL system.

Symbols.gov- Individuals can update their information by logging into their Symbols.gov user accounts utilizing their login.gov credentials.

Symbols Royalty- Corporation or Individuals can access their information by successfully logging into the portal.

7.2. What are the procedures for correcting inaccurate or erroneous information?

Job Corp- There are no procedures due to individuals not having access to their information.

Symbols.gov- Individuals are responsible for correcting their own information by logging into the website and/or calling the Symbols.gov administrator to correct their information as requested.

Symbols Royalty- Vendors (corporations and individuals) are responsible for correcting their own information by logging into the website and updating themselves.

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

Job Corp- N/A



Privacy Impact Assessment

Symbols.gov- Symbols.gov does not correct personal information. If the customer needs to change their information, they must log in to their account and make the changes. If there is a problem updating their information, there is a number they can call to request assistance.

Symbols Royalty- Symbols Royalty does not correct personal information. If the customer needs to change their information, they must log in to their account and make the changes.

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

Job Corp- N/A

Symbols.gov- If the customer needs to change their information, they must log in to their account and make the changes. If there is a problem updating their information, there is a number they can call to request assistance.

Symbols Royalty- If the vendor needs to change their information, they must log in to their account and make the changes.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: The potential risk is the inability of users to access and modify data.

Mitigation: Where applicable, individuals can correct their information by successfully logging into their account and making the changes.

Section 8 Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

NRE FS JARVIS is assessed annually against National Institute of Standards and Technology (NIST) security and privacy controls (800-53 Rev 5) at a moderate security baseline in accordance with policies and procedures established by the Forest Service and USDA. Additionally, components of NRE FS JARVIS provided by Microsoft Azure Government Software as a Service (SaaS), FedRAMP accredited cloud resources that allow secure cloud storage, sharing and collaboration are assessed annually in accordance with FedRAMP requirements.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

NRE FS JARVIS defines procedures for granting users access to the system. User access control is provided by means of role-based permissions. Access to the system requires users to authenticate and be authorized to access the respective system. Quarterly and annual account reviews are conducted. Role-based access controls, encryption, account management procedures and auditing through Azure Sentinel.



Privacy Impact Assessment

Symbols.gov: All users have public access through the website to complete and purchase orders. Users are required to login through login.gov.

8.3. How does the program review and approve information sharing requirements?

Information sharing requirements are documented, reviewed, and approved as part of the Interconnection Security Agreement (ISAs) review process.

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

Job Corp- Annual security awareness training is conducted which is required for all employees and contractors. Volunteers receive Rules of Behavior (RoB) and Privacy awareness information as part of the account request process.

Symbols.gov- Annual security and privacy awareness training is conducted which is required for all FS employees and contractors.

Symbols Royalty- Annual security and privacy awareness training is conducted which is required for all FS employees and contractors.



Privacy Impact Assessment

Approval Signatures:

Zahid Chaudhry
Forest Service
United States Department of Agriculture

Forest Service Privacy Officer
United States Department of Agriculture

Benjamin Moreau
Forest Service
United States Department of Agriculture

Officer of the Chief Privacy Officer
United States Department of Agriculture



Privacy Impact Assessment
