

Privacy Impact Assessment

for

NRE FS Joint Azure Resource Virtualized Information System (NRE FS JARVIS)

Policy, E-Government and Fair Information Practices

Version: 1.1

Date: June 22, 2023

Prepared for: USDA FS OCIO





Contact Point

Zahid Chaudhry

System Owner

USDA Forest Service

503-808-2440

Reviewing Official

Cynthia Ebersohn

Privacy Officer

USDA Forest Service

386-301-4060

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 is used by the public (symbols.gov only). The only applications in the NRE FS JARVIS that include PII are Job Corp and Symbols.gov. A2Z Cloud Dashboard and DSO Portal do not have PII. NRE FS JARVIS inherits most technical controls from Azure SaaS.

FISMA Children and / or Components

For the purposes of the Security Assessment and Authorization, the scope of the NRE FS JARVIS GSS includes hosted applications. All security controls for the hosted applications are documented and tested by NRE FS JARVIS. The following bullets summarize the key NRE FS JARVIS components.

- Job Corps

NRE FS JARVIS centralizes and securely stores data collected from the twenty-four Job Corps Centers across the US, and National Office. The solution captures, tracks

and reports information collected on student volunteers, agency and community missions and fire support. The information is collected daily and provides mission critical value to internal staff and management up to the USDA Secretary. Information collected in the application is used to fill a number of mandated reporting requirements. These include the FS1800-16 Volunteers and Partners Accomplishments, Youth Veterans Employment Programs as well as other volunteer related activities, fire support and suppression activities, volunteer and resource hours, and provides valuable information to the Department of Labor (DOL), USDA, and Congress in their decision-making processes.

- A2Z Cloud Dashboard

The A2Z Cloud Dashboard is a one stop shop for the cloud environment information on Health, Security, Consumption and Optimization. The information is divided into several sections including Outages, Security Alerts, General Alerts and Issues; Security and Health; Traffic; Cloud Consumption and Optimization. This dashboard allows executives to have a single pane of glass to monitor the health, security, and cost of their cloud environment as well as the ability to optimize that environment.

- DSO Portal

DSO Portal is a website that allows individuals to request an account within USDA NRE DevSecOps, familiarize themselves with the DevSecOps approach, learn about source code management and continuous integration as well as working with continuous delivery tools.

- Symbols.gov

The 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. On the symbols.gov website users can shop from these items for purchase through pay.gov or manually via purchase order.

Legal Authority: This system is regulated by privacy laws, regulations, and government requirements, including 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); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); Office of Management and Budget (OMB) Memos M-03-22, M-10-22, M-15-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

Job Corp- 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.

1.2 Source

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

Job Corp- 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- General public enter their own information at their discretion while purchasing their orders or upon request, an USDA Partner can aide the general public in submitting an order over the phone.

1.3 Justification

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

Job Corp- Information collected in the application is used to address several mandated reporting requirements. These include the FS1800-16 Volunteers and Partners Accomplishments, Youth Veterans Employment Programs, as well as other volunteer related activities, fire support and suppression activities, volunteer, and resource hours, and providing valuable metrics information to Department of Labor (DOL), USDA, and Congress in their decision-making processes.

Symbols.gov collects name information to ensure that shipments are sent to the correct person based on the information the person provides to purchase educational and promotional materials about conservation and wildfire prevention using Woodsy Owl, Smokey Bear and the Junior Ranger programs.

1.4 Collection

How is the information collected?

Job Corp- 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 general public in submitting an order over the phone.

1.5 Validation

How will the information be checked for accuracy?

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.

1.6 Authority

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

Job Corp- The legal authority to collect information comes from 20 CFR Part 686 – the Job Corps Under Title I of the Workforce Innovation and Opportunity Act (reference here: <https://www.law.cornell.edu/cfr/text/20/part-686>).

Symbols.gov- 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 (note)): 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 (note)): 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."

1.7 Risk Mitigation

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

Job Corp- The risk of attacks or unauthorized access attempts on the application and its database are mitigated through protection mechanisms including firewalls, antivirus software, role-based user access, and FIPS 140-2 compliant encryption. Job Corp is password protected, and data is maintained in physical locations accessible only to authorized personnel. Job Corp data is controlled through the Job Corp application interface. Individual users do not have individual database accounts, nor do they have access to any Job Corp raw database accounts. Access to Job Corp is limited only to authorized and approved users who have access to the FS Intranet Access to the Job Corp system is granted by the system administrator. There are no guest/anonymous and temporary accounts for Job Corp. In addition, all PII data is encrypted in Job Corp.

Symbols.gov- Limiting viewing of the individual user information by only the individual user and/or the support of a government admin user in Symbols.gov. Only authorized and authenticated users can access the system and this information is not used for any other purpose, other than the purposed described.

Section 2.0 Uses of the Information

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

2.1 Usage

Describe all the uses of information.

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.

2.2 Analysis and Production

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

Job Corp- Contains built-in reports used to analyze data. No other tools are used to retrieve and analyze data. PII data is used to record volunteer and fire related activities by authorized government users to generate reports.

Symbols.gov- There is no tool to analyze the data. PII data is used for transactions where individuals purchase items on the website. PII data is available to authorized government users to pull user reports in shipping out items the individuals ordered.

2.3 Commercial/Public Use

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

NRE FS JARVIS does not use any external sources of PII.

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.

Job Corp- Information is secured and protected through requiring the use of a PIV LincPass card, and a user defined personal identification number for access. Access is granted based on the position the individual holds, such as, end user or system administrator.

Symbols.gov- Login.gov and role-based access controls.

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?

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

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

3.2 Approval

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

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"

Symbols.gov- "1380- Information Collection"

3.3 Risk Mitigation

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



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

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?

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 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.

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.

NRE FS JARVIS stores and transmits purchase transactions with potential PII to Treasury systems for the purpose of processing the payments. NRE FS JARVIS does not modify or use this for any other purpose and is considered as the system of record. Similarly, credit card information is transmitted to Treasury systems for the purpose of processing the payments.

5.3 Delivery and Security Measures

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

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).

5.4 Risk Mitigation

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

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 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.)

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

Symbols.gov- [USDA/FS-19](#)

6.2 Individual Notification

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

Job Corp- N/A

Symbols.gov- This is an E-commerce website where people know they must provide the requested information to complete the purchasing and delivery of products.

6.3 Right to Decline

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

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.

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?

Job Corp- N/A



Symbols.gov- No, www.symbols.gov is an e-commerce site, and we do not share customer information with anyone.

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.

Job Corp- N/A

Symbols.gov- N/A

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?

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 are able to update their information by logging into their Symbols.gov user accounts utilizing their login.gov credentials.

7.2 Correction

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.

7.3 Notification

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

Job Corp- N/A

Symbols.gov- Symbols.gov does not correct personal information. If the customer needs to change their information, they have to 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.

7.4 Redress Alternatives

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

Job Corp- N/A



Symbols.gov- The customer will have to call the Symbols.gov customer service number for assistance.

7.5 Risk Mitigation

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

Job Corp- N/A

Symbols.gov- There are no threats identified. If there is one, customers will be notified via email.

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?

NRE FS JARVIS defines procedures for granting users access to the system. User access control is provided by means of role-based permissions.

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

8.2 Contractor Access

Will Department contractors have access to the system?

Job Corp- The contractor that developed Job Corp will continue to have system access to control and perform any updates or changes to the application.

Symbols.gov- N/A

8.3 Privacy Training

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

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- N/A

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).

NRE FS JARVIS has an ATO signed in January 4, 2022.

8.5 Audit and Technical Safeguards

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

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.

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?

Negligible privacy risks exist and are adequately addressed via current technical and security access controls.



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 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.

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?

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: 2023.07.17 11:26:08
-07'00'

Zahid Chaudhry
JARVIS System Owner (SO)
Forest Service
United States Department of Agriculture

Approval Signature

CAROLINE
GARDINER

Digitally signed by
CAROLINE GARDINER
Date: 2023.07.17 14:14:03
-05'00'

Cynthia Ebersohn
Forest Service CIO Privacy Officer
USDA Forest Service Chief Information Office

BENJAMIN
MOREAU

Digitally signed by BENJAMIN
MOREAU
Date: 2023.07.24 11:44:07
-04'00'

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