

Privacy Impact Assessment (PIA)

Inter-American Foundation (IAF)

Enterprise Network and Software Applications (EN)

System Security Program

December 2014



A. GENERAL SYSTEM/APPLICATION INFORMATION**1. Person completing this form:**

Name	Rajiv Jain
Title	Chief Information Officer
Organization	Inter-American Foundation
Address	1331 Pennsylvania Ave. NW, Suite 1200 North Washington, DC 20004
Phone Number	(202) 803-61 07
Email Address	Rjain@iaf.gov

2. System owner:

Name	Lesley Du ncan
Title	Chief Operations Officer
Organization	Inter-American Foundation
Address	1331 Pennsylvania Ave. NW, Suite 1200 North Washington, DC 20004
Phone Number	(202) 688-3047
Email Address	Lduncan@iaf.gov

3. What is the name of this system?

JAF Enterprise Network and Software Applications (EN).

4. Briefly describe the purpose of this system. What agency function does it support?

The Inter-American Foundation (IAF) is an independent federal micro-agency whose primary function consists of grant-making and the related research, evaluation, and dissemination activities benefiting poor communities in Latin America and the Caribbean.

The Enterprise Network and Software Applications (EN) include all the information systems, in use, for the mission-centric and administrative support functions of the Inter-American Foundation.

A key software application that EN supports is the Grant Evaluation Management System (GEMS). GEMS is a mission-supportive application that processes Sensitive but Unclassified (SBU) information. All IAF initiated grants are entered and tracked in GEMS and its information is used to provide reports to OMB, US Congress, American embassies, and foreign embassy representatives. The system components of GEMS and the data in it are located and operated in the secure facility of IAF.

In addition to GEMS that directly supports its mission essential functions, IAF also has utilizes other software applications in support of its administrative and management functions. While the system components and data of many of these software applications are located within IAF's facility, a few of the same are also located in other federal agency data centers that provide shared services to IAF and in secure contractor operated data centers. All such data centers are protected through FISMA compliant system security standards, tools and practices.

5. Note below whether this Privacy Impact Assessment supports a proposed new system or a proposed modification to an existing system.

This privacy impact assessment is in support of the IAF systems that are in operation. Few modules are undergoing modifications.

B. PRIVACY ACT APPLICABILITY

1. Does this system collect, maintain, or disseminate personal information in identifiable form (e.g., name, social security number, date of birth, home address, etc.) about individuals?

Yes; this system collects such information for payroll processing and health benefits.

Being a micro-agency IAF uses the information system of another US Federal agency on a shared services model, for its payroll processing and health benefits.

The personal information is collected in paper forms and then stored on the secure file servers of IAF. Access to this is restricted to the HR staff and the Chief Operating Officer of IAF. Subsequently to collecting and verifying the data they send it in an encrypted form to the agency that provides shared services to IAF.

The IAF web browsers and work stations connected IAF's computer networks, are used to access the data as they remain resident on the shared services provider's information system.

2. **If yes, will the data be retrieved by an individual's name or other personal identifier (e.g., social security number, badge number, etc.)?**

Yes; the data will be retrieved using personal identifier; but such retrieval is limited to access of the information stored on the facility of the shared service provider. The data stored on IAF's file servers are not accessed using personal identifier.

C. INFORMATION COLLECTION APPLICABILITY

1. **Will the personal data be collected from or maintained by persons who are not Federal employees?**

Yes, in addition to the personal data of federal employees, IAF utilizes college and graduate-school level interns, whose information is collected and stored.

2. **Will the data be collected from Federal contractors?**

Yes.

3. **If the answer is yes to either question 1 or 2, will the data be collected from 10 or more persons during a calendar year?**

It is unlikely that the IAF could end up collecting data from 10 or more persons during a calendar year.

4. **If the answer is yes to question 3, is the information to be collected covered by an existing OMB clearance number? If yes, indicate the clearance number**

The operation of IAF is authorized by United States Code 22, Section 290f, titled Inter-American Foundation Act.

D. RECORDS RETENTION AND DISPOSAL SCHEDULE APPLICABILITY

Does this system already have a NARA-approved records disposition schedule?

Yes

If yes, list the records schedule number

N1-454-00-001, GRS 3.13 (NC1-GRS-81-2 item 14a), N1-454-02-003.

E. SYSTEM DATA INFORMATION

1. **Type of information maintained in the system**

- a. **Describe the information to be maintained in the system (e.g., financial, medical, training, personnel.) Give a detailed description of the data.**

The name, date of birth, address and social security number are collected to process payroll for IAF employees and to report their wages to state and federal agencies for tax purposes.

For providing health benefits the name, date of birth and social security number of applicable dependents of IAF employees are also collected.

2. **Source of the data in this system**

- a. **Is data being collected from the subject individual? If yes, what types of data are being collected?**

Yes; data is being collected from subject individuals- IAF employees.

The name, date of birth, address and social security number are collected to process payroll for IAF employees and to report their wages to state and federal agencies for tax purposes.

For providing health benefits the name, date of birth and social security number of applicable dependents of IAF employees are also collected.

- b. **Is data on this individual being collected from other IAF files and databases for this system? If yes, identify the files and databases.**

No

- c. **Is data on this individual being collected from a source or sources other than the subject individual and IAF records? If yes, what is the source and what type of data is being collected?**

No data is collected from a source other than the subject individual.

- d. **How will data collected from sources other than the subject individual or IAF records be verified as current, accurate, and complete?**

N/A; no data is collected from a source other than the subject individual.

3. **Attributes of the data**

- a. **Are the data elements described in detail and documented? If yes, what is the name of the document? Where is it located? Please attach a copy to this form.**

The data elements are stored in the database of the shared service provider's information system. The shared servicer's system documentation contains a description of the data elements.

b. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes; the use of the data is both relevant and necessary for payroll processing and health benefits.

c. Will the system derive (i.e., create) new data or create previously unavailable data about an individual through aggregation from the information collected?

No; the system does not create new data about an individual.

(1) How will aggregated data be maintained, filed, and utilized?

N/A; the system does not create new data about an individual.

(2) How will aggregated data be validated for relevance and accuracy?

N/A; the system does not create new data about an individual.

4. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

All the data collected is encrypted during transmission using secure socket layer and transport security techniques.

While in storage on the shared service provider's systems, the data is stored in secure databases behind firewalls.

Access to the data from IAF work stations is restricted using role based access control techniques.

In addition, these access privileges of IAF employees are periodically reviewed and modified, to ensure that only those who must have access to fulfill their functions

5. How will the data be *retrieved* from the system?

**a. Can it be retrieved by personal identifier?
If yes, explain.**

Data can be retrieved using name, birthdate and/or social security numbers from the information system of the shared service provider.

b. Is a password or data description required?

All access to the data requires passwords.

6. Describe the report or reports that can be produced from this system.

a. What reports are produced from the system?

Reports to track manage and troubleshoot payroll processing and health benefits are produced from the system of the shared service provider.

b. What are the reports used for?

The reports are used to track, implement and troubleshoot the payroll processing and health benefits.

c. Who has access to these reports?

Only the IAF employees and federal government shared service provider employees working with IAF's payroll processing and health benefits access these reports.

7. Capability to monitor individuals

a. Will this system provide the capability to identify, locate, and monitor (e.g., track, surveillance) individuals?

No.

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

N/A; monitoring capabilities are not supported.

8. Coverage under Existing Privacy Act System of Records

a. Under which Privacy Act System of Records (SOR) notice does this system operate (link to list of SOR available on IAF website. Provide number and name.

IAF does not retrieve data using personal identifier from its own systems. Such retrieval is limited to the access of information system provided by the shared service provider. Hence as per OMB guidance an SOR is not required for IAF.

- b. If the Privacy Act System of Records is being modified, will the SOR notice require amendment or revision?**

N/A.

9. Access to the Data

- a. Who will have access to the data in the system (users, managers, system administrators, developers, other)?**

Access is restricted to few IAF's employees in charge of payroll processing and health benefits.

- b. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?**

IAF's code of conduct, employment agreements, system use notice on the login screens and standard operating procedures describe these.

- c. Will users have access to all data in the system or will users' access be restricted? Explain.**

Data sensitivity is taken into account for providing access. All access to sensitive parts of the data is restricted to few IAF's employees in charge of payroll processing and health benefits.

- d. What controls are or will be in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

IAF's code of conduct, employment agreements, system use notice on the login screens and standard operating procedures provide the necessary controls to deter prevent and detect misuse.

- e. Do other systems share data or have access to data in this system?**

Other than the shared service provider agency, no other agency has access to the data in this system.

- f. Will other agencies share data or have access to data in this system (Federal, State, local, other)?**

None

If yes, explain how the data will be used by the other agency.


Other than the shared service provider agency, no other agency has access to the data in this system.

- g. Were Privacy Act clauses cited (or will be cited) and were other regulatory measures addressed in contracts with contractors having access to this system?**

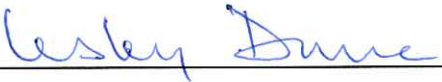
Privacy act and FIS MA requirements are a part of all IAF contracts.

D. APPROVAL OF PRIVACY IMPACT ASSESSMENT

1. Information Technology Security Specialist

 (Signature) 15 Dec 2014 (Date)
Daniel Glenn, Chief Information Security Officer

2. Chief Operations Officer /Senior Agency Official for Privacy

 (Signature) 12/12/2014 (Date)
Lesley Duncan, Chief Operations Officer