Privacy Impact Assessment (PIA)

Inter-American Foundation (IAF)

Enterprise Network (EN)

June 2021
A. GENERAL SYSTEM/APPLICATION INFORMATION

1. Person completing this form:

<table>
<thead>
<tr>
<th>Name</th>
<th>Danny Glenn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>Organization</td>
<td>Inter-American Foundation</td>
</tr>
<tr>
<td>Address</td>
<td>1331 Pennsylvania Ave. NW,</td>
</tr>
<tr>
<td></td>
<td>Suite 1200 North Washington, DC 20004</td>
</tr>
<tr>
<td>Phone Number</td>
<td>202-688-3053</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:dglenn@iaf.gov">dglenn@iaf.gov</a></td>
</tr>
</tbody>
</table>

2. System Owner:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lesley Duncan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Chief Operating Officer (COO) / Chief Privacy Officer (CPO)</td>
</tr>
<tr>
<td>Organization</td>
<td>Inter-American Foundation</td>
</tr>
<tr>
<td>Address</td>
<td>1331 Pennsylvania Ave. NW,</td>
</tr>
<tr>
<td></td>
<td>Suite 1200 North Washington, DC 20004</td>
</tr>
<tr>
<td>Phone Number</td>
<td>202-688-3047</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:lduncan@iaf.gov">lduncan@iaf.gov</a></td>
</tr>
</tbody>
</table>

3. What is the name of this system?

   Enterprise Network (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 benefitting poor communities in Latin America and the Caribbean.

The Enterprise Network (EN) is a general support system that includes the network infrastructure as well as information systems in use for mission-centric and administrative support functions of the Agency located in Washington, D.C. A list of business functions performed/supported by EN include:

1. User authentication and authorization
2. File server and services for storage and collaboration
3. Network access to a shared service for time and attendance application
4. Human Resource (HR) functions
5. Legal and Freedom of Information Act (FOIA)
6. Financial reports
7. Federal regulatory and compliance applications
8. Access to email
9. Access to internet

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 existing EN general support system (GSS) that is operational. Several system components 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.

   Personal information is collected on forms or scanned identification documents and stored on the secure IAF file server on a restricted shared drive.

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; Scanned forms will be retrieved based on an individual’s name such as “firstnamelastname” followed by the form name (e.g., OF 306, driver’s license, Emergency Notification form).
C. INFORMATION COLLECTION APPLICABILITY

1. Will the personal data be collected from or maintained by persons who are not Federal employees?
   - No; Personal data is maintained by IAF federal employees.
   - Yes; IAF utilizes college and graduate school level interns whose employment acceptability forms are stored/maintained.

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 the 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.

D. RECORDS RETENTION AND DISPOSAL SCHEDULE APPLICABILITY

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

For Intern Acceptability Package Information:
National Archives and Records Administration (NARA) General Records Schedule (GRS) 2.1: Employee Acquisition Records

For Emergency Notification Form Information:
NARA GRS 5.3: Continuity and Emergency Planning Records, Item 020 (DAA-GRS-2016-0004-0002)
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.

IAF HR maintains/stores 2 distinct types of PII:

(1) Emergency Notification Form – IAF may collect limited information about emergency contacts or next of kin from agency personnel. This information may include the following:
   - Name;
   - Contact Information (e.g., address, phone number); and
   - Relationship to IAF personnel or individual associated with the Agency.

(2) Intern Employment Acceptability Package – Interns must complete the Optional Form (OF) 306 “Declaration for Federal Employment” as well as provide acceptable forms of Identification in accordance with Identity Proofing requirements for USAccess Personal Identity Verification (PIV) credentials. This information may include the following:
   - General Personal Data (e.g., name, date of birth, place of birth, citizenship, maiden name, alias, phone numbers, military service)
   - Identifying Numbers (e.g., social security, driver’s license, passport, permanent resident, alien registration)

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 collected from subject individuals:
   - IAF personnel;
   - Interns.

Types of data collected include:
   - General Personal Data (e.g., name, date of birth, place of birth, citizenship, maiden name, alias, phone numbers, military service); and
   - Identifying Numbers (e.g., social security, driver’s license, passport, permanent resident, alien registration).
b. Is data on this individual being collected from other 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?

Not Applicable; 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.

Data elements maintained are defined as part of the types of data collected in question 2a above.

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

Yes.

Emergency Notification Form Information – In working to achieve the agency’s mission, there may be instances such as an emergency, incident, or other event that requires someone to reach out to an employee’s designated emergency contact or next of kin.

Intern Employment Acceptability Package Information – These forms and documents are required in order for the intern to be employed/work at the agency. Copies of these forms and documents are maintained by HR in the case that the intern decides to re-intern with the agency the following year.

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?

Not Applicable; the system does not create new data about an individual.

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

Not Applicable; 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?

IAF PII data is consolidated only in the sense of where it is stored (i.e., EN protected file server on a restricted shared drive). IAF HR regulates and controls access to PII stored on the shared drive. Only IAF HR and the COO have access to PII.

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

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

   Yes.
   Scanned forms with PII will be retrieved based on an individual’s name such as “firstnamelastname” followed by the form name (e.g., OF 306, driver’s license, Emergency Notification form).

b. Is a password or data description required?

   All access to PII requires IAF user logon identification and authentication (i.e., password).

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

a. What reports are produced from the system?
   No reports are produced from this system.

b. What are the reports used for?
   Not Applicable

c. Who has access to 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. The system does not provide the capability to locate, identify, surveil or track individuals.
   
b. What controls will be used to prevent unauthorized monitoring?
   
   Not Applicable: 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.
   
   A SORN is currently in the process of being published.
   
b. If the Privacy Act System of Records is being modified, will the SOR notice require amendment or revision?
   
   Not Applicable

9. **Access to the Data**
   
a. Who will have access to the data in the system (users, managers, system administrators, developers, other)?
   
   Only IAF Human Resources and the COO have access to PII data that resides on an EN file server in an access restricted shared drive location.
   
b. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?
   
   Procedures, controls and responsibilities regarding PII access within the system have been documented with the EN System Security Plan (SSP).
   
c. Will users have access to all data in the system or will users' access be restricted? Explain.
   
   Access to PII is restricted to only IAF Human Resources and the COO. HR controls and maintains access to the restricted PII share drive on the EN
file server.

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?

No.

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.

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

Privacy Act and FISMA requirements are a part of all IAF contracts.
F. APPROVAL OF PRIVACY IMPACT ASSESSMENT

1. Information Technology Security Specialist

   Danny Glenn, CISO
   Signature: Date 28 June 2021

2. Chief Operations Officer/Chief Privacy Officer

   Lesley Duncan
   Signature: Date

   Lesley Duncan, COO