INTER-AMERICAN FOUNDATION

Privacy Act of 1974; System of Records

AGENCY: Inter-American Foundation.

ACTION: Notice of a new system of records.

SUMMARY: The Inter-American Foundation (IAF) proposes to add three new electronic systems of records: IAF/FPPS (Federal Personnel and Payroll System) (IAF-01), IAF Salesforce CRM (Customer Relationship Management) (IAF-02), IAF GovGrants (IAF-03). This notice is required to meet the requirements of the Privacy Act to publish in the Federal Register a notice of the existence and character of records maintained by the agency.

DATES: This action will be effective without further notice on [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*] unless comments are received that would result in a contrary determination. Comments must be received by [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Comments should include the system name the comments relate to and may be submitted electronically to PrivacyActRequests@iaf.gov or by mail to Chief Information Officer, Inter-American Foundation, 1331 Pennsylvania Ave, NW; Suite 1200, Washington, DC 20004.

FOR FURTHER INFORMATION CONTACT: Dominic Bumbaca, Chief Information Security Officer, Inter-American Foundation, 1331 Pennsylvania Ave, NW; Suite 1200, Washington, DC 20004, at (202)-360-4530.

SUPPLEMENTARY INFORMATION: The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals; these records are maintained in a “system of records,” which refers to a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular

assigned to the individual. The Privacy Act requires each agency to publish in the Federal Register a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. In accordance with 5 U.S.C. 552a(r), the IAF has provided a report of these system of records to the Office of Management and Budget (OMB) and to Congress. The IAF is adding three new systems of records.

The Federal Personnel and Payroll System (FPPS) (IAF-01) is an online personnel and payroll system providing support to Federal agency customers through DOI's Interior Business Center (IBC). FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. IAF uses FPPS to manage human resources and payroll functions; ensure proper payment for salary and benefits; track time worked, leave, or other absences for reporting and compliance purposes; and meet regulatory requirements. FPPS allows for immediate updates and edits of personnel and payroll data. IAF has contracted with DOI IBC for human resource services including the use of FPPS. This SORN covers only the Inter-American Foundation data held within FPPS and does not cover the data of any other agencies utilizing DOI IBC's services nor does it cover data belonging to DOI.

The IAF Salesforce CRM system (IAF-02) is used to manage relationships with potential or current contacts, beneficiaries, partners, donors, and other civil society organizations. It supports the mission of the Agency by increasing transparency, improving outreach, communications, and collaboration efforts with our stakeholders, as well as employing sound, repeatable methodologies.

The IAF GovGrants system (IAF-03) will provide the agency a web-based full life-cycle grants management system. The system will maintain grant program information, notice of funding opportunities, agency award application package information, agency award agreement, and reporting information to meet compliance requirements with the Data Act and Foreign Assistance Act.

SYSTEM NAME AND NUMBER:

IAF/FPPS (Federal Personnel and Payroll System), IAF-01

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

(1) The system is located and managed at U.S. Department of the Interior, Interior Business Center, Personnel and Payroll Systems Division, 7301 West Mansfield Ave, MS D-2400, Denver, CO 80235-2230.

(2) Temporary paper records are also located at the IAF Headquarters, located at 1331 Pennsylvania Avenue N.W. Suite 1200, North Washington, DC, 20004.

SYSTEM MANAGER:

Chief Information Officer (CIO), Inter-American Foundation, 1331 Pennsylvania Ave NW #1200, Washington, DC 20004, (202)-360-4530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 5101, et seq., Government Organization and Employees; 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans; 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers; and Public Law 101-576 (Nov. 15, 1990), the Chief Financial Officers (CFO) Act of 1990.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system is to manage personnel and payroll functions, to ensure proper payment for salary and benefits, track time and attendance, leave, and other absences for reporting and compliance purposes; and facilitate reporting requirements to other Federal agencies, including

the Department of the Treasury and the Office of Personnel Management, for payroll, tax, and human capital management purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THIS SYSTEM:

Individuals covered by the system include current and former IAF employees for Federal employment. This system may also include limited information regarding employee spouses, dependents, emergency contacts, beneficiaries, or estate trustees who meet the definition of "individual" as defined in the Privacy Act.

CATEGORIES OF RECORDS IN THIS SYSTEM:

This system maintains records including:

Employee biographical and employment information: Employee name, other names used, citizenship, gender, date of birth, age, group affiliation, marital status, Social Security number (SSN), truncated SSN, legal status, place of birth, records related to position, occupation, duty location, security clearance, financial information, medical and family leave information, disability information, education information, driver's license, race, ethnicity, personal or work telephone number, personal or work email address, military status and service, home or mailing address, Taxpayer Identification Number (TIN), bank account information, professional licensing and credentials, family relationships, involuntary debt (garnishments or child support payments), employee common identifier (ECI), organization code, user identification and any other employment information.

Salary and benefits information: Salary data, retirement data, tax data, deductions, health benefits, allowances, insurance data, Flexible Spending Account, Thrift Savings Plan information and contributions, pay plan, payroll records, awards, court order information, back pay information, debts owed to the government as a result of overpayment, refunds owed, or a debt referred for collection on a transferred employee.

Timekeeping information: Time and attendance records, and leave records.

This system may also contain correspondence, documents and other information required to administer payroll, leave, and related functions.

RECORD SOURCE CATEGORIES:

Information is obtained from individuals on whom the records are maintained, official personnel records of individuals on whom the records are maintained, supervisors, timekeepers, previous employers, the Internal Revenue Service and state tax agencies, the Department of the Treasury, other Federal agencies, courts, state child support agencies, employing agency accounting offices, and third-party benefit providers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures that are 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 to authorized entities determined to be relevant and necessary outside IAF as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) IAF;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any IAF employee or former employee acting in his or her official capacity;

(4) Any IAF employee or former employee acting in his or her individual capacity when IAF or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The United States Government or any agency thereof, when DOJ determines that IAF is likely to be affected by the proceeding.

B. To the Department of the Treasury or other Federal agency as required for payroll purposes, for preparation of payroll and other checks and electronic funds transfers to Federal, State, and local government agencies, non-governmental organizations, and individuals.

C. To the Department of the Treasury, Internal Revenue Service, and state and local tax authorities for which an employee is or was subject to tax regardless of whether tax is or was withheld in accordance with Treasury Fiscal Requirements, as required.

D. To the Office of Personnel Management or its contractors in connection with programs administered by that office, including, but not limited to, the Federal Long Term Care Insurance Program, the Federal Dental and Vision Insurance Program, the Flexible Spending Accounts for Federal Employees Program, and the electronic Human Resources Information Program.

E. To another Federal agency to which an employee has transferred or to.

F. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law--criminal, civil, or regulatory in nature.

G. To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office.

H. To Federal, State or local agencies where necessary to enable the employee's to obtain information relevant to the hiring or retention of that employee, or the issuance of a security clearance, contract, license, grant or other benefit.

I. To appropriate Federal and state agencies to provide reports including data on unemployment insurance.

J. To the Social Security Administration to credit the employee or emergency worker account for Old-Age, Survivors, and Disability Insurance (OASDI) and Medicare deductions.

K. To insurance carriers to report employee election information and withholdings for health insurance.

L. To charitable institutions when an employee designates an institution to receive contributions through salary deduction.

M. To the Department of the Treasury, Internal Revenue Service, or to another Federal agency or its contractor, to disclose debtor information solely to aggregate information for the Internal Revenue Service to collect debts owed to the Federal Government through the offset of tax refunds.

N. To any creditor Federal agency seeking assistance for the purpose of that agency implementing administrative or salary offset procedures in the collection of unpaid financial obligations owed the United States Government from an individual.

O. To any Federal agency where the individual debtor is employed or receiving some form of remuneration for the purpose of enabling that agency to collect debts on the employee's behalf by administrative or salary offset procedures under the provisions of the Debt Collection Act of 1982.

P. To the Department of the Treasury, Internal Revenue Service, and state and local authorities for the purpose of locating a debtor to collect a claim against the debtor.

Q. To the Federal Retirement Thrift Investment Board's record keeper, which administers the Thrift Savings Plan, to report deductions, contributions, and loan payments.

R. To the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services, for the purposes of locating individuals to establish paternity; establishing and modifying orders of child support; identifying sources of income; and for other child support enforcement actions as required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

S. To an expert, consultant, grantee, or contractor (including employees of the contractor) of IAF that performs services requiring access to these records on IAF's behalf to carry out the purposes of the system, including employment verifications, unemployment claims, W-2 processing services, leave and earning statements, and 1095-C Affordable Care Act statements.

T. To the Office of Personnel Management Employee Express, which is an employee self-service system, to initiate personnel and payroll actions and to obtain payroll information.

U. To the Department of Labor for processing claims for employees, emergency workers, or volunteers injured on the job or claiming occupational illness.

V. To Federal agencies and organizations to support interfaces with other systems operated by the Federal agencies for which the employee is located, for the purpose of avoiding duplication, increasing data integrity and streamlining government operations.

W. To another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

X. To the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

Y. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

Z. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, regarding the issuance of a security clearance, license, contract, grant or other benefit.

AA. To state, territorial, and local governments, and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

BB. To the Department of the Treasury to recover debts owed to the United States.

CC. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of IAF or is necessary to demonstrate the accountability of IAF'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.

DD. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained.

EE. To other Federal agencies and organizations to provide payroll and personnel processing services under a shared service provider cross-servicing agreement for purposes relating to IAF cross-servicing agreement for purposes relating to IAF payroll and personnel processing.

FF. To the Office of Personnel Management, the Merit System Protection Board, Federal Labor Relations Authority, or the Equal Employment Opportunity Commission when requested in the performance of their authorized duties.

GG. To state offices of unemployment compensation to assist in processing an individual's unemployment, survivor annuity, or health benefit claim, or for records reconciliation purposes.

HH. To Federal Employees' Group Life Insurance or Health Benefits carriers in connection with survivor annuity or health benefits claims or records reconciliations.

II. To any source from which additional information is requested by IAF relevant to a IAF determination concerning an individual's pay, leave, or travel expenses, to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested.

JJ. To the Social Security Administration and the Department of the Treasury to disclose pay data on an annual basis, and as necessary to execute their statutory responsibilities for the effective administration of benefits programs, payroll and taxes.

KK. To a Federal agency or in response to a congressional inquiry when additional or statistical information is requested relevant to a Federal benefit or program.

LL. To the Department of Health and Human Services for the purpose of providing information on new hires and quarterly wages as required under the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

MM. To appropriate agencies, entities, and persons when:

(1) IAF suspects or has confirmed that there has been a breach of the system of records;

(2) IAF has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, IAF (including its information systems, programs, and operations), the Federal Government, or national security; and

(3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IAF's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

NN. To another Federal agency or Federal entity, when IAF determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(1) Responding to a suspected or confirmed breach; or

(2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

OO. To an agency or organization 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.

PP. To a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of discovery, pursuant to appropriate court order or other judicial process in the course of criminal, civil or administrative litigation.

QQ. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

RR. Disclosure to Consumer Reporting Agencies: Disclosure pursuant to 5 U.S.C. 552a (b)(12). Disclosures may be made from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or federal Claims Act of 1996 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained and stored electronically by IBC. Temporary paper records are maintained in file folders stored within a locked filing cabinet within IAF Headquarters in a secure facility and secure office area with controlled access.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

FPPS authorized users, including IAF authorized personnel, may retrieve records by employee name, Social Security Number (SSN), Tax Identification Number (TIN), employee common identifier (ECI), birth date, or assigned person number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL:

Records are maintained in accordance with NARA approved record schedules for the retention of reports and data. Specifically, General Records Schedule (GRS) 1.0 “Finance” and GRS 2.0 “Human Resources” are applicable to the FPPS system.

The system generally maintains temporary records, and retention periods vary based on the type of record under each item and the needs of the agency. Paper records are disposed of by shredding.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

During normal hours of operation, paper records are maintained in a locked file cabinet in a secured office area inside a secure facility under the control of authorized personnel. Paper records are shredded in accordance with Government data destruction standards

To prevent misuse, (e.g., unauthorized browsing) IAF signed an Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) with the IBC to clearly establish and document IBC and client security roles and responsibilities. Most of the employee data in FPPS is collected from individuals and entered into FPPS by an authorized Agency human resources professional with access to the system.

The FPPS system has undergone a formal Security Authorization and Accreditation and has been granted an authority to operate by the DOI in accordance with FISMA and NIST standards. FPPS is rated as FISMA Moderate based upon the type of data, and it requires strict security and privacy

controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

Data is protected by the following electronic security systems: Password, Firewall, Encryption, User ID, Intrusion Detection System, Virtual Private Network (VPN), Public Key Infrastructure (PKI) Certificates, Personal Identity Verification (PIV) Card.

RECORD ACCESS PROCEDURES:

An individual requesting records on himself or herself must send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS" and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which the individual is seeking records.

CONTESTING RECORD PROCEDURES:

An individual requesting the correction or removal of material from his or her records should send a signed, written request to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR CORRECTION" and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which a change is requested, and 3) clearly state the correction requested and provide any supporting information available.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST INQUIRY" and 1) must be signed by the individual, 2) must name or otherwise clearly describe the system of records on which the individual is seek information about, and 3) should clearly state the requester's relationship with the IAF and timeframe (ex. former IAF employee from 2020-2021) to facilitate the location of any applicable records.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Not applicable.

SYSTEM NAME AND NUMBER:

IAF Salesforce CRM, IAF-02

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

The IAF Salesforce CRM application is hosted in the Salesforce Government Cloud. The physical location and technical operation of the system is at the Salesforce Government Cloud's Chicago (Elk Grove Village, IL) and Washington (Ashburn, VA) data centers.

SYSTEM MANAGER:

Chief Information Officer (CIO), Inter-American Foundation, 1331 Pennsylvania Ave NW #1200, Washington, DC 20004, (202)-360-4530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

22 U.S.C. 290f, 44 U.S.C. 3101, *et seq.*

PURPOSE(S) OF THE SYSTEM:

The Salesforce customer relationship management (CRM) system will serve as the agency's contact and relationship managing platform of record. It will provide the agency with a cost-effective, user-friendly, cloud-based, single, integrated platform solution to better engage our contacts, partners and other stakeholders by facilitating access to contact information, simplifying workflows, improving annual reporting and internal and external communications.

CATEGORIES OF INDIVIDUALS COVERED BY THIS SYSTEM:

Individuals covered by the system include donors, partners, and other stakeholders, including U.S. agencies, foundations, private sector, academia, not-for-profit organizations, Congress, IAF staff alumni, fellows, board members, current staff, and interns.

CATEGORIES OF RECORDS IN THIS SYSTEM:

This system contains information needed for customer engagement to facilitate the agency mission. This system maintains records including: Full name, Account Name, Account Physical Business, Address, Account Mailing Business Address, Title, Business Email address, Phone, Mobile Phone, Gender, Optional links to social networking profiles, Call Notes, Description of Partnerships and prospective partnerships.

RECORD SOURCE CATEGORIES:

The sources for information in the system are the individuals about whom the records are maintained. This may include business cards that are provided by the individual or official contact information. Furnishing of the information is voluntary.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures that are 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 to authorized entities, as is determined to be relevant and necessary, outside IAF as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office, made at the written request of the constituent about whom the record is maintained.

b. To the National Archives and Records Administration (NARA) for records management purposes.

c. To Agency contractors, grantees, consultants, or experts who have been engaged to assist the agency in the performance of a Federal duty to which the information is relevant.

d. To a Federal, State, local, foreign, or tribal or other public authority, on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

e. To the Office of Management and Budget (OMB) when necessary to the review of private relief legislation pursuant to OMB circular No. A–19.

f. To designated Agency personnel for the purpose of performing an authorized audit or oversight evaluation.

g. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Government Accountability Office (GAO), or other Federal agencies when the information is required for program evaluation purposes.

h. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency 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 IAF or another agency or entity) that rely upon the compromised information; (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IAF's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

i. In any criminal, civil or administrative legal proceeding, where pertinent, to which IAF, a IAF employee, or the United States or other entity of the United States Government is a party before a court or administrative body.

j. To an appeal, grievance, hearing, or complaints examiner; an equal employment opportunity investigator, arbitrator, or mediator; and/or an exclusive representative or other person authorized

to investigate or settle a grievance, complaint, or appeal filed by an individual who is the subject of the record.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained and stored electronically in encrypted format within the Salesforce Government cloud controlled environment and accessed only by authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information may be retrieved by account name, individual name, or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL:

Records are maintained and disposed of in accordance with NARA approved record schedules, specifically, General Records Schedule (GRS) 6.5 “Public Customer Service Records”, Item 20 and DAA–GRS2017–0002–0002.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The Salesforce Government Cloud Plus system achieved a provisional Authority to Operate (ATO) at the “High” impact level issued by the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB). System access is limited to IAF authorized users utilizing multi-factor authentication.

IAF Salesforce CRM has configurable, layered data sharing and permissions features to ensure users have proper access. Authorized users have access only to the data and functions required to perform their job functions. Role based access is managed via IAF Salesforce administrators using Salesforce system administration, user, and security functions. PII information in the system will be encrypted and stored in place, and HTTPS protocol will be employed in accessing Salesforce.

RECORD ACCESS PROCEDURES:

An individual requesting records on himself or herself must send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked “PRIVACY ACT REQUEST FOR ACCESS”

and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which the individual is seeking records.

CONTESTING RECORD PROCEDURES:

An individual requesting the correction or removal of material from his or her records should send a signed, written request to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR CORRECTION" and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which a change is requested, and 3) clearly state the correction requested and provide any supporting information available.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST INQUIRY" and 1) must be signed by the individual, 2) must name or otherwise clearly describe the system of records on which the individual is seek information about, and 3) should clearly state the requester's relationship with the IAF and timeframe (ex. former IAF employee from 2020-2021) to facilitate the location of any applicable records.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Not Applicable

SYSTEM NAME AND NUMBER:

IAF GovGrants, IAF-03

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

The IAF GovGrants application will be hosted in the FedRAMP-authorized Salesforce Government Cloud Plus U.S. designated data center environment(s). Authorized IAF personnel (staff and contractors) and external proponents and grantees (foreign and domestic) will access IAF's electronic grant management system via an online web portal. IAF Headquarters is located at 1331 Pennsylvania Ave NW #1200, Washington, DC 20004. The IAF Salesforce CRM application is hosted in the Salesforce Government Cloud. The physical location of the Salesforce Data Center is currently 7600 Doane Drive, Manassas, VA 20109.

SYSTEM MANAGER:

Chief Information Officer (CIO), Inter-American Foundation, 1331 Pennsylvania Ave NW #1200, Washington, DC 20004, (202)-360-4530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

22 U.S.C. 290f*;* 44 U.S.C. 3101, *et seq.;* DATA Act, Public Law 113–101; Foreign Assistance Act, Public Law 87-195.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to provide the agency a web-based full life-cycle grants management system. This will allow IAF to centrally manage the grants process and provide the capability to manage grant applications, reviews, issue progress reports, make obligations and disbursements, record site visits, communicate with grantees and proponents, approve or reject amendment requests, and hold other oversight documents. The IAF awards small grants to civil society organizations primarily in Latin America and the Caribbean, that support inclusive economic prosperity, reduce food insecurity, combat corruption, promote safety and security, protect the environment and build resilience to natural disasters, and sustainably manage natural resources.

CATEGORIES OF INDIVIDUALS COVERED BY THIS SYSTEM:

IAF employees, IAF contractors, individuals ("Representatives") representing entities applying for or receiving IAF support including support in the form of a grant, cooperative agreement, partnership agreement, equity agreement, or other IAF financed agreement ("Awardees"), and key

individuals of Awardees (“Key Individuals”) who are expected to primarily be responsible for the administration of, control, or benefit from IAF support. Almost all of the information for non-Federal individuals included in this system will be of non-U.S. citizens.

CATEGORIES OF RECORDS IN THIS SYSTEM:

This system maintains the following records on individuals:

IAF Employee full names, titles, phone numbers, email addresses;

IAF Contractor full names, titles, phone numbers, email addresses;

Representative full names, titles, organization mailing address, phone numbers, email addresses. In situations where the Awardee's bank account lists a Representative as a recipient on the account, bank account information related to the account is collected including bank name, SWIFT code, and bank account number.

Key Individual full names (including any aliases or variations of spelling), titles, type of Government-issued identification, Government-issued identification number, Countries of origin and citizenship, birthdates, and certifications.

RECORD SOURCE CATEGORIES:

The primary sources of information in the system are the Representatives who directly input information about their Awardees. Information may also be obtained directly from IAF employees or contractors. Additionally, information will originate from the System for Award Management (SAM.GOV) (GSA/GOVT-9).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

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 IAF as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of State when it is necessary to conduct a check under Section 487 of the Foreign Assistance Act.

B. To the Department of Justice (DOJ), including Offices of the United States Attorneys, or other federal agency conducting litigation, or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. IAF or any department thereof;

2. Any employee or former employee of IAF in their official capacity;

3. Any employee or former employee of IAF in their individual capacity when the department of Justice or IAF has agreed to represent the employee; or

4. The United States or any agency thereof.

C. 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.

D. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

E. To an agency or organization 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.

F. To appropriate agencies, entities, and persons when (1) IAF suspects or has confirmed that there has been a breach of the system of records; (2) IAF has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, IAF (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IAF's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

G. To another federal agency or federal entity, when IAF determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding

to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

H. 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, when 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.

I. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for IAF, when necessary to and 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 IAF officers and employees.

J. To an individual's employer or affiliated organization to the extent necessary to verify employment or membership status.

K. To the news media and the public, with the approval of the Chief Privacy Officer 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 IAF or is necessary to demonstrate the accountability of IAF'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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained and stored electronically in encrypted format within the Salesforce Government Cloud Plus controlled environment and accessed only by authorized personnel.

IAF maintains records in this system in an electronic database and a digital file repository.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

IAF staff may retrieve records in this system by grantee/applicant name, organization representative, email address, application number, award number, report number, and disbursement number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL:

Records are maintained and disposed of in accordance with NARA approved record schedules, specifically, General Records Schedule (GRS) 1.2 “Grant and Cooperative Agreement Records”, Item 10 and DAA–GRS2013–0008–0007, Item 20 and DAA-GRS2013-0008-0001, Item 21 and DAA-GRS-2013-0008-0006, Item 22 and DAA-GRS2103-0008-0002, and Item 30 and DAA-GRS-2013-0008-0003.

IAF otherwise maintains records in GovGrants on an indefinite basis for reference purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The Salesforce Government Cloud Plus system achieved a provisional Authority to Operate (ATO) at the “High” impact level issued by the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB). System access is limited to IAF authorized users utilizing multi-factor authentication.

IAF GovGrants has configurable, layered data sharing and permissions features to ensure users have proper access. Authorized users have access only to the data and functions required to perform their job functions. Role based access is managed via IAF GovGrants administrators using Salesforce system administration, user, and security functions. PII information in the system will be encrypted in transit and at rest, and HTTPS protocol will be employed in accessing GovGrants. Multi-factor authentication is required to access the system and data stored in the system of record is also protected by a firewall and intrusion detection.

RECORD ACCESS PROCEDURES:

An individual requesting records on themselves must send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS" and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which the individual is seeking records.

CONTESTING RECORD PROCEDURES:

An individual requesting the correction or removal of material from their records should send a signed, written request to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR CORRECTION" and must: 1) be signed by the individual, 2) name or otherwise clearly describe the system of records in which a change is requested, and 3) clearly state the correction requested and provide any supporting information available.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on themselves should send a signed, written inquiry to the System Manager at PrivacyActRequests@iaf.gov or the physical address above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST INQUIRY" and 1) must be signed by the individual, 2) must name or otherwise clearly describe the system of records on which the individual is seek information about, and 3) should clearly state the requester's relationship with the IAF and timeframe (ex. former IAF employee from 2020-2021) to facilitate the location of any applicable records.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Not Applicable

Natalia Mandrus,
Associate General Counsel

[FR Doc. 2024-20595 Filed: 9/10/2024 8:45 am; Publication Date: 9/11/2024]