

Privacy Impact Assessment
Office of Chief Financial Officer
ERP Financials

I. System Identification

- 1) IT System Name: ERP Financials
- 2) IT System Sponsor: Deron Burba, OCIO Director of Modernization
- 3) Unit Sponsor: Alice Maroni, Chief Financial Officer
- 4) IT System Manager: Huyen Tran
- 5) PIA Author: Deron Burba
- 6) Date: December 2009
- 7) Brief (one paragraph) description of the system:

The Enterprise Resource Planning (ERP) Financials system is the financial and procurement management system supporting the internal operations of the Institution. To support the operations of the Institution, the ERP Financials system integrates with the GSA GovTrip travel management system to record obligations and process payments for official travel for staff and members of the public that are invited to travel on behalf of the Institution. The system is also used to record financial obligations and to process payments related to stipends provided for certain academic appointments.

II. Privacy Assessment

- 1) What information is being (or will be) collected.

The ERP Financials system collects and maintains the following information:

- Contact information including name, address, telephone, and fax numbers
- Banking information including bank routing code and bank account number necessary to support electronic funds transfers
- Identifying numbers including DUNS and Tax Id Number (TIN)
- Social Security Number when vendor information is for an individual or a sole proprietor that utilizes their individual SSN as their TIN.
- Payment Information including date, amount, and method of payment

2) Why the information is being collected.

The information is being collected to enable recording obligations to individuals, organizations, or corporations; enable payments related to these obligations via Treasury Check or Treasury EFT; and to enable reporting to the Internal Revenue Service (IRS) when required. Information about members of the public is being collected for individuals invited to travel on behalf of the Institution.

3) What the intended use of the information.

To maintain information to necessary to document the obligations of the Institution, enable the initiation of payments such as travel reimbursements, and when appropriate, reporting to the IRS.

4) With whom the information will be shared.

The information is used internally by Smithsonian staff involved in the processing of obligations and payments. Payments to vendors meeting IRS requirements for reporting are shared with the IRS and a Form 1099 or 1042s is supplied to the individual or organization.

5) What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared.

All information is collected directly from the individual or their designee by staff within the Smithsonian. In the event the information is shared with the IRS a Form 1099 or 1042s is provided to the individual or corporation.

6) How the information will be secured.

The ERP Financials system contains controls to protect sensitive data from unauthorized access and/or disclosure, assure integrity of data stored in electronic form, and to protect data from unauthorized alteration or modification. The system is controlled with respect to access, authority to modify, and ability to operate.

The ERP Financials system includes subsystems that are accessible to authorized users. Each user is assigned to a unique user logon ID and password. The subsystems enforce a strong password policy and accounts are automatically locked after three failed login attempts. The passwords are stored in encrypted form. The systems require users to change their password every 90 days. Access is revoked when a person leaves or changes jobs.

The servers supporting these systems are physically protected in a secure computer room, where access is limited to authorized personnel. The servers are on a subnet within the Smithsonian's network that is protected by a dedicated

firewall providing a restrictive security policy. The applications are accessed by users via web browsers and utilize Secure Sockets Layer (SSL) encryption. All backups are retained for a limited time period and kept off-site in a secure facility with limited, controlled access. All backup tapes sent offsite are encrypted.

ERP Financials systems are certified and accredited using guidance contained in NIST Special Publication 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*.

The Smithsonian's certification and accreditation program is based on a risk assessment and testing of controls commensurate with the importance and sensitivity of the system and acceptance of risk and authorization to operate by the program sponsor and the Chief Information Officer.