

**U. S. Department of Commerce
National Oceanic and Atmospheric Administration
Information Systems Management Office**



**NOAA Non-Core
Commerce Business System (CBS)
NOAA 1101**

PRIVACY IMPACT ASSESSMENT STATEMENT

March 2008

NOAA Non-Core Commerce Business System (CBS)

Unique Project Identifier: 006-48-01-01-01-3801-00
(NOAA 1101)

Project Description:

In October 2002, NOAA successfully migrated its legacy accounting system to the Commerce Business System (CBS) as its official financial system of record. CBS is the integrated financial management system of record throughout the Department of Commerce. Core CBS consists of the Core Financial System (CFS) interfaced with standard Commerce-wide administrative systems for procurement (CSTARS), bankcards, time reporting and labor cost distribution, data warehouse, and CCR.

CBS enables Commerce and NOAA to meet the requirements of the [Chief Financial Officers Act](#) (CFOs Act) of 1990, P.L. 101-576; the [Federal Managers' Financial Integrity Act of 1982](#), P.L. 97-255 (31 U.S.C. 3512 et seq.); and Office of Management and Budget (OMB) [Circular A-127](#), Financial Management Systems. CBS supports the financial functions required to track financial events, provide financial information important for the financial management of Commerce and its operating units, and required for the preparation of financial statements, and to allow Commerce to continue receiving clean financial audit opinions.

NOAA Non-Core CBS financial systems modules support NOAA Permanent Change of Station (PCS - Relocation Manager), Travel Manager, and other activities (NOAA data warehouse) that are unique to NOAA and/or are not yet part of the Commerce CBS/CFS. Similar Non-Core CBS modules are located at the Census Bureau and National Institute of Standards and Technology (NIST).

The NOAA Non-Core CBS System is hosted in the NOAA Information Technology Center (ITC). The ITC is operated by the Office of the Chief Information Officer/Information Security Management Office (OCIO/ISMO) Financial and Administrative Computing Division (FACD). In addition to the NOAA Non-Core CBS, FACD supports NOAA's current accounting system and other major administrative systems, and the development of new accounting and administrative systems when needed.

To streamline Commerce financial management processes and realize cost savings, CBS is currently considering consolidating all server infrastructures to provide one hardware platform. The CBS server consolidation effort will increase standardization and optimization opportunities and is a key component of Commerce's strategic infrastructure consolidation plans.

1. What information is to be collected (e.g., nature and source)?

Both Privacy Act / personally identifiable information (PII) and business identifiable information (BII) are collected by the Non-Core CBS Systems. This information is

needed for the purposes of reimbursing employees for travel expenses by direct payment using bank routing and account information, verification of business payment information via the government-wide Central Contractor Registration (CCR), and for contract payments using bank routing and account numbers. PII data includes full name as identified in the Personnel/Payroll system, Social Security Number (SSN) used in the PCS system, and home address.

BII collected information includes the Taxpayer Identification Number (Employer Identification Number), the Data Universal Numbering System (DUNS) numbers and financial institution information specific for payments to NOAA contractors or businesses providing goods or services to NOAA, including bank routing number and bank account number.

2. Why is the information being collected (e.g., to determine eligibility)?

The information is collected solely for the payment of travelers (employees and invitational travelers), and for reporting on employee / vendor payments.

- a. A Taxpayer Identification Number (TIN) is a nine-digit number, which is either an Employer Identification Number (EIN) assigned by the Internal Revenue Service (IRS) or a Social Security Number (SSN) assigned by the Social Security Administration (SSA). The SSN identifies an individual and Employer identification Number (EIN) identifies a business. A “sole proprietor” business may use the SSN as the identifier. Agencies are required to collect TINs [[Debt Collection Improvement Act, 31 U.S.C. 7701\(c\)](#)] and to include the TIN in vouchers submitted for payment [[31 U.S.C. 3325 \(d\)](#)]. This information is required in support of tax processing (W2s and 1099s), determination of entitlements (relocation of sufficient distance and reimbursement based on number of dependants and their age, etc).
- b. Name is needed to identify an individual and business, and is also part of the criteria to identify a vendor to determine eligibility for registration in the CCR.
- c. Date of birth further supports the process of determining entitlement reimbursements for dependants of relocating employees.
- d. Address is used to validate entitlements related to distance moved for relocated employees.
- e. Bank routing and account numbers enable direct payment after identification of the payee.

3. What is the intended use of the information (e.g., to verify existing data)?

The information is used to ensure that financial transactions are conducted in a timely and correct manner, to protect against fraudulent transactions, and to generate and maintain financial management data adequate to meet acceptable accounting and auditing standards. Entitlement determination and tax processing also require this information.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

Financial information is shared with the [Treasury Financial Management Service](#) (FMS) to issue payments to employees and companies doing business with NOAA. Employee reimbursements are also shared with the Internal Revenue Service as part of income tax reporting (IRS 941 process).

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how may individuals grant consent?

All employees submitting travel claims are apprised of the use of this information, and that it is used solely for verification and payment. At the point of entry into CCR or other systems, a business or individual is advised by that system's owner of the right to refuse to provide the information requested and how this will affect them.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls

The Financial Systems Division (FSD) of the NOAA Finance Office reviews application updates, system updates, and security updates weekly and performs rigorous testing on platforms dedicated to this purpose. Upon completion of successful testing, the ITC is notified to allow scheduling of system updates or patches, or FSD schedules application updates, as appropriate. Both FSD and the ITC use configuration change management processes to assure management and technical oversight and review. Hardcopy reports that contains PII data is maintained in locked cabinets. Any proposed user of the non-core CBS applications must be authorized by the employee's supervisor in writing, and recertified each year to maintain their access.

Operational Controls

The NOAA 1101 computer systems are located at the NOAA Information Technology Center (ITC) in Landover, Maryland. The ITC data center has a uniformed guard service, video cameras covering entrances, and active monitoring by the Silver Spring (Security) Command Center 24x7, as well as key card controls limiting access to all production servers. Nightly backups are performed with backup media being stored approximately 17 miles from the production servers in a fire-proof media safe. Integrity checks of the backups are performed weekly. Data is restricted to the least number of users that requires access to the information. The applications are not accessible to the public, and any user must be authorized to have access to the application.

Technical Controls

Access controls are implemented on production systems through the use of system usernames and passwords as well as database (application) usernames and passwords. NOAA 800-53R1 access controls are enforced for access to all non-core CBS applications. Access logs are kept and reviewed for any anomalies. Password length and duration of validity follow Department of Commerce standards as outlined in the *IT Security Program Policy and Minimum Implementation Standards*.

A Security Certification and Accreditation (C&A) in accordance with the requirements of the [Federal Information Security Act of 2002](#) (FISMA) was completed for this system on March 29, 2007. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years.

Please describe your process for logging/monitoring database extracts, including the process for reviewing the logged information to determine: 1) how it is used, and 2) if there is still a need for it after 90 days (such extracts must be destroyed after 90 days if no longer needed). If the logging/monitoring process is automated, please describe the process used for implementing [NIST-800-53 Rev 1](#), Security Controls for Auditable Events (AU-2, "Auditable Events", AU-3, "Content of Audit Record", AU-6, "Audit Monitoring, Analysis and Reporting" and AU-11, "Audit Record Retention"). Please include the requirement to verify that PII extracts are logged, verified and erased within 90 days in the auditable events criteria in AU-2 and AU-11.

The non-core CBS applications, Travel Manager and Relocation Manager, are Progress DBMS-based applications. These applications do not directly support a database extract by end-users. The Travel Manager application does not contain Privacy Act data; however, it does contain PII data. In those cases where an extract must be generated, the Progress DBA develops the extract routine and generates the data, provides the appropriate non-disclosure notices, and formally transmits the data to the requesting party. Currently, this logging process is entirely manual. In those cases where an extract that contains PII or BII data is required, the extract is tracked via manual entry and a determination is made up front to verify the duration of the extracted data. A notice is provided that the data must be destroyed after 90 days if it is no longer required. The manual logs of who currently has extracted PII data are reviewed monthly.

The Relocation Manager application does contain Privacy Act and PII data; however, access to this application and its data is limited to less than 15 authorized NOAA Finance Office users. In those cases where an extract must be generated, the Progress DBA develops the extract routine and generates the data, provides the appropriate non-disclosure notices, and formally transmits the data to the requesting party. Currently, this logging process is entirely manual. In those cases where an extract that contains PII or Privacy Act data is required the extract is tracked via manual entry and a determination is made up front to verify the duration of the extracted data. A notice is provided that the

data must be destroyed after 90 days if it is no longer required. The Relocation Manager application generates a monthly and an annual file extract of W2 and IRS 941 related information. This data includes employees' SSN and income related information. As part of the IRS 941 and W2 process this information is generated from the application as a file and used as part of NOAA's formal IRS reporting procedures. This data is retained as part of official IRS submissions by NOAA and the IRS. No additional logging beyond the IRS 941 and / or the W2 submission process is maintained for these electronic data transmissions.

Beginning in Q4-FY08, for any PII/BII extracts from Travel Manager or Relocation Manager that have not been destroyed after 90 days, an email will be sent requiring written/email confirmation that either the PII/BII data has been destroyed or that the need continues for an additional 90 days. Data extracts sent to Treasury for disbursement of funds or for IRS reporting via W2 or 941 processing are exempt from this tracking requirement since this data is required by law and these organization must retain this information.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No. The existing Privacy Act system of records notice for [DEPT-2, Accounts Receivable](#), applies to the personal information in this system.

8. Are these records covered by an approved records control schedule?

The retention period for these records is guided by the [General Records Schedules \(GRS\)](#), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with [GRS 20, item 3](#), electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. [GRS 6, item 1](#) authorizes the disposal of the equivalent paper copies six years and three months after the period covered by the account, **EXCEPT:** Accounts and supporting documents pertaining to American Indians are not authorized for disposal. Such records must be retained indefinitely since they may be needed in litigation involving the Government's role as trustee of property held by the Government and managed for the benefit of Indians.

Program Contact: Joseph C. Smith
Ph: (301) 763.6300x141 or Joseph.C.Smith.III@noaa.gov