March 27, 2008

PRIVACY IMPACT ASSESSMENT (PIA)
FOR THE
U.S. DEPARTMENT OF COMMERCE (DOC)
ECONOMIC DEVELOPMENT ADMINISTRATION (EDA)

WebCIMS Correspondence Tracking System
Implemented in an EDA - Specific Configuration

Project: WebCIMS

Unique Project Identifier: N/A

OMB information collection control number: N/A

Privacy Act System of Records: N/A

Project Description:

WebCIMS (Case and Issues Management System) provides a means for maintaining records on important, sensitive, and/or time critical correspondence, both EDA/DOC external and internal. WebCIMS is a commercial off-the-shelf (COTS) software product implemented in an EDA-specific configuration to provide an effective method for managing correspondence by tracking not only the original item, but also the response and/or actions taken by management or staff.

Purpose Statement:

EDA staff in Headquarters (Washington, DC) or in the six regional offices (Philadelphia, Atlanta, Chicago, Denver, Austin, and Seattle) may receive correspondence from other EDA offices, DOC Office of the Secretary, other DOC operating units, Congress, the White House, or from other sources. This correspondence and the follow-up routing steps, replies, signatures, etc., must be tracked to ensure that documentation is not lost and deadlines are met. In addition, EDA staff may receive correspondence, solicited or unsolicited, from the public. This correspondence must also be tracked until the issue is resolved. EDA implemented this EDA-specific configuration of WebCIMS to accomplish this need. WebCIMS serves as an agent between the EDA organization and EDA's customers and/or constituents.

1. <u>What law or regulation authorizes the collection and maintenance of the information?</u>

The collection and maintenance of this information is authorized by the Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373).

2. What information is being collected, maintained, or disseminated (identify the data as Personally Identifiable Information or Business Identifiable Information)?

The type of personal information contained in WebCIMS could include names, home addresses, home phone numbers, and e-mail addresses. Both personally identifiable information and business identifiable information may be included in the collection. The information collected is pertinent to the stated purpose for which the information is to be used, and only information that is required for responding to correspondence is collected and stored.

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

The information is shared within EDA with authorized parties only. There is no other agency involved.

4. What opportunities will individuals have (if any) to decline providing information in the case of voluntary collections?

The WebCIMS system is not an information collection within the meaning of the Paperwork Reduction Act (PRA); individuals who correspond with EDA are not required to provide information. However, individuals who contact EDA and request a response must provide the basic information needed for a reply. Failure to provide the information may render it impossible for EDA to correspond with the requestor. Requestors who do not expect a reply may decline to provide their contact information, and no reply will be provided.

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

The information will be secured via both administrative and technological controls. WebCIMS is covered by an approved Certification and Accreditation (C&A) package that includes a system security plan and a risk assessment. The potential risk of inappropriate disclosure and/or unauthorized disclosure is mitigated by:

- limiting the number of authorized system users;
- requiring an access form signed by a supervisor prior to issuance of a user ID;
- requiring the use of passwords;
- employing logical edit checks for event sequencing;
- providing initial and annual system security training;
- monitoring authorized user activity;
- notification of unauthorized system access or usage to the system administrator; and
- documenting user violations and following up with appropriate remedial action.

The data resides on a network that employs a secure firewall providing intrusion monitoring and detection audit logging. Changes to the software must follow configuration management controls.

Buildings employ security systems with locks and access limits. The hardware that stores the data resides in a server room accessible only to authorized personnel, and employing environmental controls. Only those individuals that have the need to know, in order to carry out their official duties, have access to the data. The computerized database is protected by passwords and access is limited. Back-ups of the data are secured off-site in fireproof safes.

Data Extract Log and Verify Requirements: In an effort to safeguard personally identifiable information (PII), the Office of Management and Budget (OMB) issued M-06-16: Protection of Sensitive Agency Information, dated June 23, 2006, and reiterated in OMB Memorandum M-07-16, dated May 22, 2007. One of the requirements is to Log all computer-readable data extracts from databases holding sensitive information, and verify each extract including sensitive data has been erased within 90 days or its use is still required. EDA does not have this process automated at this time. EDA's Office of Information Technology is researching tools to perform this capability. To satisfy this requirement in the interim, EDA has implemented a manual process to log computer-readable data and verify requirements.

WebCIMS only provides an ad hoc query capability which is controlled via the application and is a COTS product. Therefore, EDA can not omit the sensitive data fields from the reporting process. If the user requests a special ad hoc query with this type of data from OIT, only the DBA or system administrators can access the data outside of the application. Only authorized OIT staff members have this level of access. The following is the manual process:

Application Reporting:

- If EDA WebCIMS system users extract PII or BII type of data and store it on the desktop/personable computer, the user must inform the OIT Development team leader.
- The Development Team leader must log the information.
- The Development Team leader will check within 90 days if the data has been erased or its use is still required when applicable. See "Log All Computer-Readable Data Extracts" log sheet.
- The user must provide the location of the file.

Note: This process will be in place by May 30, 2008

Ad Hoc Query Via OIT

- User must submit an ISD Action Request form for data extract.
- OIT staff member must log the request if the data extracted contained PII or BII information.
- The Development Team leader will check within 90 days if the data has been erased or its use is still required when applicable.

6. Name, e-mail address, and telephone number of a contact person:

Sandranette Moses, smoses@eda.doc.gov, 202-482-2463