Privacy Impact Assessment
for the

Accounting Package (ACCPAC)

DHS/FEMA/PIA-024

June 8, 2012

Contact Point
Cheryl Ferguson
Office of Chief Financial Officer
Federal Emergency Management Agency
(540) 504-1783

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency's (FEMA) Office of the Chief Financial Officer (OCFO) Debt Establishment Unit (DEU) owns and operates the Accounting Package (ACCPAC) application. ACCPAC is a commercial off the shelf (COTS) product that assists FEMA Accounts Receivable personnel track, monitor, and manage debts owed to the Agency. FEMA is conducting this PIA because ACCPAC collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) including Employer Identification Numbers (EIN) and Social Security Numbers (SSN) to perform its tasks.

Overview

ACCPAC assists FEMA Accounts Receivable with tracking, monitoring, and managing debts owed to the Agency. These debts can include erroneous disaster support payments to citizens, overpayment of travel reimbursement to employees, excessive payment to a grantee, and restitution from individuals that have defrauded the Agency. To achieve this, ACCPAC collects PII such as EIN or SSN in order to aid the Agency in recovering these debts. FEMA staff manually enter debt information into ACCPAC after referencing Integrated Financial Management System (IFMIS)[1] and National Emergency Management Information System (NEMIS) Emergency Support Module (both legacy NEMIS systems), and Department of the Treasury (Treasury) Financial Management Service (FMS) into the Debt Management System (FedDebt[2]).

There are three specific modules of ACCPAC: 1) Accounts Receivable; 2) Contact Master; and 3) Common Services. The Accounts Receivable Module is used to create customer accounts; post invoices, receipts, credit memos, and debit memos; and run and post monthly interest and penalty charges. The Contact Master Module is used to track debt and account status; document any contact with each debtor through the use of comments and notes; view debtor's posted transactions and receipts as individual line items; provide current account balance; and run the customer detail report which shows all activity on the account. Last, the Common Services Module allows authorized users to reverse payments which have been rejected for insufficient funds or debited.

The Accounts Receivable module maintains the information manually input from IFMIS, legacy NEMIS, FedDebt and/or U.S. Courts. This information is used to create the account in ACCPAC. The other two modules then use the information populated in the Accounts Receivable module to track debt, account status, and generate reports within ACCPAC.

Information within ACCPAC is provided to the Treasury FMS when debts become delinquent in order for Treasury to pursue debt collection on behalf of FEMA. Treasury FMS has

[1] IFMIS-Merger PIA, *available at:* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_ifmis_merger.pdf.
[2] FedDebt PIA, *available at*: http://www.fms.treas.gov/pia/feddebt_pia.pdf.

multiple databases and a greater ability to collect debts owed by individuals, especially through the Internal Revenue Service (IRS) with income tax offsets. Treasury FMS identifies all collections by their unique identifying number: social security number (SSN) for individuals, and employer identification number (EIN) for organizations. The delinquent debts are entered manually in an Excel spreadsheet which is uploaded through a Treasury FMS site into FedDebtfor further collection efforts as described in the Federal Claims Collection Act. In order for Treasury FMS to offset eligible federal monies, an EIN or SSN is needed to make a match within FedDebt.

The FEMA/OCFO/ Accounts Receivable Debt Establishment Unit (DEU) receives Bill for Collection (BFC) requests from U.S. Courts and various FEMA program offices. BFCs can come in the form of U.S. Postal Mail and via email in password-protected documents. The information that DEU receives from FEMA program offices is entered manually into IFMIS and ACCPAC. DEU staff query the system by name, SSN or TIN to determine if the debtor has an existing account in ACCPAC. If no account exists, then one is created using the information provided in the BFC request. If an account already exists, then DEU verifies all fields and makes any necessary updates to the current information. After the debtor account is created or located, an invoice is generated.

Debts are also established in ACCPAC from information extracted from legacy NEMIS. The data is provided in two methods either through the FEMA Operational Data Store (ODS)/Enterprise Data Warehouse (EDW),[3] which houses all of the legacy NEMIS data, and scripts are automatically generated into a report for use for the FEMA Accounts Receivable staff; or through an actual interface between NEMIS and the main financial system IFMIS in which the data is then manually obtained from IFMIS to be keyed/posted into ACCPAC. The match criterion for NEMIS and ACCPAC is the NEMIS registration ID number. It should be noted that ACCPAC does not interface with any other system.

If FEMA/OCFO/ Accounts Receivable Receipts Unit (RU) receives payment, a search for debtor information in ACCPAC is conducted. Once the record is located, the RU determines how the payment is going to be applied between administrative fees, penalties, interest, and principal; in that order. A distribution code is obtained within the system. Once the entire deposit transaction has been completed, a receipt entry transaction occurs.

If FEMA does not receive payment or if no response is received, and no contact is made between the individual and FEMA/OCFO/ Accounts Receivable/Debt Management Unit (DMU) on average between 60 to 180 days, a Letter of Intent (LOI) is sent to the individual. The LOI notifies the individual that their information, including PII, may be transmitted to Treasury FMS for further collection and reporting to credit bureaus. DMU shares this information via encrypted electronic transmission. Once Treasury FMS processes the transmitted information, they send DMU a control number which becomes part of the individual's record in ACCPAC.

[3] Any IT system that houses PII data within the Enterprise Data Warehouse will have its own PIA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authority for this system is based on the Joint Financial Management Improvement Program (JFMIP), other statutes, Executive Orders, Office of Management and Budget (OMB) and Treasury guidance, regulations, and DHS and FEMA policies:

- *Debt Collection Act of 1982 as amended, 31 U.SC. § 3717;*
- *Federal Claims Collection Act, 31 U.S.C. § 3711, et seq.;*
- *31 C.F.R. parts 900 - 904;*
- *Federal Records Act, 44 U.S.C. § 2901 et seq., and chapters 21, 25, 31, and 33 of this title, 44 U.S.C. § 2101 et seq., 3101 et seq., and 3301 et seq.;*
- *Robert T. Stafford Disaster Relief and Emergency Assistance Act (P. L. 100-707);*
- *Homeland Security Act of 2002 (P. L. 107-296);*
- *Federal Managers' Financial Integrity Act of 1982 (P. L. 97-255);*
- *Chief Financial Officers Act of 1990 (P. L. 101-576);*
- *Federal Financial Management Improvement Act of 1996 (P. L. 104-208);*
- *Executive Order 9397;*
- *Executive Order 13478;*
- *OMB Circular A-127;*
- *OMB Circular A-129;*
- *OMB Circular A-130;*
- *The Internal Revenue Code, 26 U.S.C. § § 6011 (b) 6109; and*
- *Department of Homeland Security Financial Management Policy FMP017; Accounting for Public Accounts Receivable and Collections.*

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information in the system is covered by the following DHS-wide SORNs:

- DHS/ALL-007 Accounts Payable System of Records, 73 FR 61880, October 17, 2008; and
- DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61885, October 17, 2008.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan (SSP) has been completed for ACCPAC dated January 13, 2011. ACCPAC is operational and was granted an Authority to Operate (ATO) on March 24, 2011 for

one year. It is currently being reviewed for reauthorization in conjunction with this PIA. ACCPAC has a "high" categorization in accordance with National Institutes of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199. The ACCPAC Sensitive Systems Policy (SSP) complies with DHS SSP Directive 4300A.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

ACCPAC uses the standards for accounting records as stated in the General Records Schedule (GRS) 6, Accountable Officers' Accounts Records.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ACCPAC is not subject to the requirements of the Paperwork Reduction Act (PRA) because there is no specific form completed by the public to populate information in ACCPAC. Information is populated in ACCPAC that is extracted from various source systems.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ACCPAC collects, uses, maintains, retrieves, and disseminates the following information:

- Customer Number;
- Customer Name;
- EIN or SSN;
- Address;
- City;
- Country;
- State/Province;
- Telephone Number;
- Zip Code;
- Fax Number;
- Email Address;
- Web Site;
- Account Information (text field not used with every record; does not contain banking information);
- Pay Status;
- Recoupment Information;
- Status;

- Vendor Number (the number that corresponds to vendor number in the main financial system, IFMIS-Merger); and
- Outstanding Balance.

2.2 What are the sources of the information and how is the information collected for the project?

Information received for debt collection purposes can arrive in a variety of formats. The information can be received directly from the individual either electronically in password protected documents by email or through the U.S. Postal Service. The information may contain PII information, such as SSNs, in order to successfully collect the debt since this information is required by Treasury FMS.

In addition, OCFO staff manually enters debt information into ACCPAC from the following applications through various methods of notification of an outstanding debt:

- IFMIS;
- NEMIS Emergency Support Module;
- U.S. Courts; and
- FedDebt.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ACCPAC does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The ACCPAC application checks information that is input into the system for duplications, completeness, and authenticity. The application developers implemented specific FEMA rules for checking the valid syntax of ACCPAC information (e.g., character set, length, numerical range, and acceptable values) are in place to verify that inputs match specified definitions for format and content. These character sets, length, numerical range, acceptable value settings are completed as part of the Excel document used for manual entry. The system itself will not allow duplication by way of specific unique customer ID numbers and other data checks before data is accepted into the database.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A privacy risk associated with this system includes receiving more information than is needed from the sources outlined in Section 2.2 to provide accounting of financial status.

Mitigation: This privacy risk is mitigated because ACCPAC is not integrated with any other system. ACCPAC is a standalone system. Information from the source systems is manually entered into ACCPACC. Any data that is extracted from ACCPAC and sent to Treasury FMS is sent through a secure Treasury FTP site and only contains the information required by Treasury FMS to perform a successful offset to collect the funds owed the government.

Privacy Risk: A privacy risk associated with this system includes collecting/using erroneous or inaccurate information.

Mitigation: This privacy risk is mitigated because ACCPAC is a standalone system and does not integrate with any other system. Any system naturally inherits the risk of inaccurate information especially when the data are entered manually. Mitigation occurs with reports that are used to reconcile aspects of the data with the various program offices to ensure that data reported in their system matches certain fields within ACCPAC, such as the original debt amount, name of the debtor, and date.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ACCPAC utilizes information provided from the sources outlined in Section 2.2 to create accounts for debts owed to FEMA. To facilitate the recoupment process, ACCPAC will require PII (e.g., full name, address, SSN, and phone) to ensure ACCPAC transactions are processed accurately. Transactional products created by ACCPAC are: invoices, cash receipts, debit, and credit memos.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, the project does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

FEMA OCFO operates ACCPAC. No other FEMA components have assigned roles and responsibilities within ACCPAC.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: A privacy risk associated with this system is that information within ACCPAC may be used in a manner inconsistent with original collection purpose.

Mitigation: This privacy risk is mitigated by monitoring the use of the system for official purposes only by the system steward and the Information System Security Officer (ISSO) in conjunction with governance information outlined in this PIA. Information collected is only those data fields necessary for processing a debt collection account in ACCPAC and ultimately to Treasury FMS for potential offset.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

ACCPAC collects information directly from the sources outlined in Section 2.2. Notice is provided by way of this PIA and the SORNs outlined in Section 1.2. Individuals are issued a Notice of Debt (NOD). If no response is received or no contact is made between the individual and FEMA or they refuse to pay the debt, a Letter of Intent (LOI) is sent to the individual notifying them that their information, including PII, may be transmitted to Treasury FMS for further collection and reporting to credit bureaus.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Information in ACCPAC is required to create receivable accounts on individuals, entitled groups, or entities, and to account for the collection of public funds. Opportunities for individuals to consent to use, decline to provide information, and opt out is facilitated through the FEMA programs and OCFO before the information is entered into ACCPAC.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: A privacy risk associated with this system includes the individual not having prior or existing notice of the collection.

Mitigation: This privacy risk is mitigated by providing notice to individuals by way of NODs and LOIs regarding the debt. Additionally, individuals are provided notice by way of this PIA and the associated SORNs in Section 1.2.

Privacy Risk: Another privacy risk associated with this system includes ACCPAC receiving information from some systems in Section 1.2 that have not been fully reviewed to determine whether or not privacy compliance documentation, including a PIA or SORN is required or is required to be updated.

Mitigation: This privacy risk is mitigated by completing this PIA and identifying the need to collect PII and addressing all risks and mitigations. Additionally, both FEMA IFMIS and Treasury FedDebt systems have published PIAs. The NEMIS Emergency Support Module is currently in the privacy development, review, and approval process.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

The data contained in ACCPAC are federal government records originally collected and maintained by the source systems listed in 2.2. Consistent with NARA and FEMA approved retention and disposal schedule GRS 7-2, records are destroyed six years and three months after the close of the fiscal year involved.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: A privacy risk associated with this system includes PII being retained for longer than necessary in ACCPAC.

Mitigation: This privacy risk is mitigated by establishing a NARA-and FEMA-approved retention and disposal schedule that must be followed by each source system outlined in Section 2.2. FEMA's policies and procedures for expunging data, including records pertaining to approved and unapproved applications, at the end of retention period are consistent with NARA and DHS policy and guidance. The procedures are documented by the FEMA Records Officer and follow NARA's GRS guidelines for both paper and electronic copies.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal Agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

ACCPAC data are extracted and sent to Treasury FMS. Treasury FMS uses the information in order to collect debts as required by the Federal Claims Collection Act. Data elements include: full name, address, EIN/SSN. EIN/SSN are used to process information within FedDebt. This information is encrypted and transmitted electronically utilizing the Treasury-mandated encryption software. These transmissions to Treasury FMS occur only to collect debts. After processing, Treasury FMS sends a control number to FEMA which becomes part of the records within the OCFO.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing of ACCPAC records is compatible with the SORNs outlined in Section 1.2 and is only done consistent with the published routine uses therein which are also compatible with the purpose for original collection.

6.3 Does the project place limitations on re-dissemination?

In accordance with the Interconnection Security Agreement (ISA) between Treasury FMS and FEMA, information shared between agencies is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with FEMA policy relating to sensitive but unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior written approval of Treasury FMS and FEMA Disclosure Offices.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

ACCPAC data is extracted and sent to Treasury FMS through Treasury's secure FTP site. Treasury FMS uses the information in order to collect debts as required by the Federal Claims Collection Act. Data elements include: full name, address, TIN/SSN. TIN/SSN are used to process information within FedDebt. This information is manually entered into an Excel spreadsheet (batches) that was specially designed by Treasury FMS. Individual debts can also be entered directly into Treasury FMS's system if there is only one or two debts to turn over to them to process. Batches are kept sequentially in the LOI batch dates log. The log begins with the batch number, date, and count that the original LOI batch was mailed. Then the log tracks the amount and count of those LOIs that are eligible to be debts certified to Treasury FMS; the date, count, amount, and electronic sequencing numbers when the batch is actually transmitted to Treasury FMS; and the count, amount, and date of what was accepted at Treasury FMS. When the file is transmitted to Treasury FMS, a reply is received of the total number of records received.

Sharing of ACCPAC records is compatible with the SORNs outlined in Section 1.2 and is only done consistent with the published routine uses therein which are also compatible with the purpose for original collection.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A privacy risk associated with this system includes unauthorized disclosure of the information in ACCPAC.

Mitigation: This privacy risk is mitigated through an ISA between Treasury FMS and FEMA. Treasury FMS and FEMA have agreed to the following:

Treasury FMS and the FEMA shall protect the data to maintain confidentiality, integrity, and availability of the data and information systems. The data and information systems will be protected in accordance with DHS SSP Directive 4300A, the NIST SP 800-53 assigned minimum security controls, and NIST FIPS 199 security categorization of both systems to ensure that the connection will be protected to the requirements of higher categorized system.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may submit a Privacy Act (PA) or Freedom of Information Act (FOIA) request to gain access to their information within ACCPAC and request that it be corrected. Redress is provided directly within ACCPAC. When these corrections and updates are made they are automatically transferred and manually updated to the systems outlined in Section 2.2.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may submit a PA or FOIA request to gain access to their information within ACCPAC and request that it be corrected. Redress is provided directly within ACCPAC. When these corrections and updates are made they are manually updated to the systems outlined in Section 2.2.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified through this PIA as well as the SORNs listed in Section 1.2 of how to correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A privacy risk associated with this system includes that individuals will be unable to obtain redress through ACCPAC due to underlying source data systems.

Mitigation: This privacy risk is mitigated by policies and procedures that require any change made within ACCPAC must also be made in underlying source data systems.

Privacy Risk: A privacy risk associated with this system includes individuals not knowing that if a correction or redress action must be made that ACCPAC needs to be amended.

Mitigation: This privacy risk is mitigated because ACCPAC manually updates the systems listed in Section 2.2 when correction or redress is made. If a redress creates a financial change, an individual or organization will be notified by a corrected bill or credit memo.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The ACCPAC system owner and those financial administrators designated are responsible for the creation of new users, assignment of roles and privileges, and ACCPAC user account management. Users of ACCPAC are identified by the establishment of a user ID

providing access to the FEMA network. The security measures for ACCPAC user-IDs are consistent with the security controls employed by the FEMA network. No one can access ACCPAC outside the FEMA network. Protection of user account information is through the FEMA network administration and the additional security layer in the ACCPAC application that authenticates users to specific roles. The OCFO also established the OCFO Internal Control Office to conduct regular reviews of ACCPAC authorized users to ensure their access aligns with the appropriate roles in the system. Likewise, the ISSO receives and reviews daily logs including failed login attempts, database users that should be removed, and super-user activity.

In addition to the system administrator, database administrator, and developer roles, OCFO employs additional separation of duties/roles within ACCPAC to ensure against fraud, waste, or abuse. The basic objective of the ACCPAC separation of duties standard is to safeguard the assets of FEMA by ensuring that no single individual has the ability to complete all the ACCPAC functions.

SOPs have been implemented to manage data extracts for systems located at the Mount Weather Emergency Operations Center (MWEOC), where ACCPAC is located. This SOP establishes procedures for personnel security, data storage, transport, sanitization and disposal, and incident reporting. Additionally, all personnel accessing ACCPAC must follow the DHS Privacy Office's Handbook for Safeguarding Sensitive PII at DHS, which applies to every FEMA employee, contractor, detailee, and consultant, and provides details of handling and/or transporting of sensitive materials to include digital and non-digital. These procedures address not only the paper and electronic outputs from systems, but also the transportation or mailing of sensitive media.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All FEMA employees and contractor personnel supporting ACCPAC are required to attain initial and refresher training in privacy awareness and information security awareness.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ACCPAC has a System Security Plan dated January 13, 2011. ACCPAC received a Certification and Accreditation (C&A) and was granted a 1-year Authority to Operate (ATO) through March 24, 2012. It is currently being reviewed for reauthorization in conjunction with this PIA.

ACCPAC system administrator personnel and support personnel go through a favorably adjudicated background investigation before gaining access to system resources. User accounts are routinely audited for levels of security required to perform job duties. The program manager and/or the COTR works with the personnel management office to facilitate the process for setting up initial identification and authentication credentials, providing assistance if credentials are lost and/or compromised, and removing access credentials upon termination or loss of need to know.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any ACCPAC system interface or information data sharing within DHS or other outside organizations will require an MOU and/or ISA reviewed by the system steward, and will be fully vetted through the FEMA IT Security Branch, FEMA Privacy Officer, and FEMA Office of Chief Counsel prior to sending to DHS for a formal review and approval.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security