

EXHIBIT G



Privacy Impact Assessment
for the

Federal Financial Management System

March 23, 2011

Contact Point

Radha Sekar

Chief Financial Officer

U.S. Immigration and Customs Enforcement

(202) 732-7560

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Federal Financial Management System (FFMS) is a web-based, workflow management and financial transaction system that provides core financial management functions for U.S. Immigration and Customs Enforcement (ICE) and five other components within the Department of Homeland Security (DHS): U.S. Citizenship and Immigration Services (USCIS), Science & Technology (S&T), the National Protection Programs Directorate (NPPD), Office of Health Affairs (OHA), and DHS Office of Management (MGMT). FFMS is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. The system contains personally identifiable information (PII) about DHS employees, contractors/vendors, customers and members of the public that participate in DHS programs. ICE is conducting this privacy impact assessment (PIA) because FFMS collects and maintains PII. This PIA focuses on ICE's collection and use of PII, and each component will publish appendices to this PIA as required to describe their collection and use of PII in FFMS.

Overview

Background

ICE's Office of the Chief Financial Officer (OCFO), Office of Financial Management (OFM) is responsible for operating and maintaining FFMS, which supports financial management activities and processes for ICE and five other DHS components, specifically, USCIS, S&T, NPPD, OHA, and MGMT. All six components use FFMS for recording and processing commitments, obligations, collections and payments (collectively "financial transactions"), which are defined as follows:

- *Commitments*: The reservation of agency funds to ensure the availability of those funds before the agency awards a contract for goods or services, or for anticipated expenditures such as payroll and contingent liabilities.
- *Obligations*: The designation of agency funds toward a legal liability or definite promise to pay for goods and services received or ordered. Examples of liabilities are: procured goods or services under a government contract, for monthly payments on a lease, government purchase card transactions, DHS employee travel or relocations, etc.
- *Collections*: Invoices sent to and payments received by the agency, often from customers (i.e., other federal, state and local agencies) for goods or services provided by the agency.
- *Payments*: Disbursements of agency funds (including reimbursements) to satisfy an obligation.

Generally, these financial transactions occur between DHS and its employees (e.g., payroll, benefits, work-related travel), contractors/vendors that provide goods and services to DHS, and customers who receive goods and services from DHS. For USCIS and ICE, FFMS financial transactions also occur with members of the public who participate in programs where the public pays fees or other payments to the agency, e.g., immigration benefit application fees, cash immigration bonds for the release of detained aliens.



Federal Financial Management System (FFMS)

FFMS is a web-based, core financial management system used to record and process financial transactions for ICE and five other DHS components. The system's primary functions include processing:

- Payroll and payroll-related transactions (e.g., health benefits and retirement) for DHS employees;
- Travel reimbursements and other personnel payments (e.g., conference attendance fees, local travel, etc.) for DHS employees and other individuals such as invitational travelers/speakers;
- Payments for contractors/vendors providing goods and services (e.g., training and purchase card services/activities) to DHS;
- Collections of debts owed to DHS, often by customers (i.e., other federal, state and local agencies) who receive services from DHS; and
- Collections of fees or other funds from the public related to the operation of a DHS program (e.g., immigration benefit application fees, posting of cash immigration bonds), and any associated reimbursements of such funds.

The system is also used to generate statistical and financial transaction reports required for reporting to the Department of the Treasury (Treasury) and other federal agencies outside DHS (e.g., Office of Management and Budget) as well as *ad hoc* reports for internal, congressional and senior management purposes.

FFMS is comprised of eight modules briefly described below:

- *Cost Management*: Used for recording and tracking costs associated with reimbursable agreements.¹ This module enables a user to track allocation costs (e.g., labor, expenses, hours, etc.).
- *Database Administrator Management*: Used to customize menus and profiles (e.g., granting screen and report access), and view the audit trail of maintenance data (i.e., the business rules that govern various procedures in FFMS) recorded in FFMS.
- *Funds Management*: Used for entering and processing commitments and obligations, and for managing and controlling funds availability checks and allocations.
- *General Ledger Management*: Used for maintaining general accounting data and processing general ledger reports and financial statements which detail current expenditures, allocations, collections and payments for reporting to DHS (e.g., CFO Reports) and the Treasury (e.g.,

¹ A reimbursable agreement means any arrangement whereby a federal agency agrees to provide goods or services to another agency in return for reimbursement of costs incurred.



Homeland Security

Privacy Impact Assessment

ICE, Federal Financial Management System (FFMS)

Page 4

Federal Agencies' Centralized Trial-Balance System [FACTS] I and II Reports).² In addition, it maintains employee personnel and payment remittance information.

- *Payroll Management*: Used for receiving and processing DHS employee payroll accounting and time and attendance information.
- *Payment Management*: Used for maintaining vendor records; processing and transmitting payment transactions to the Treasury; and recording financial transactions to update the general ledger with the proper accounts payable and related expense amounts.
- *Receipts Management*: Used for maintaining customer records; generating customer invoices and credit memos (in the event of an overpayment to DHS); processing customer payments and miscellaneous cash receipts issued to customers for services provided by DHS. In addition, it records transactions to update the general ledger with proper accounts receivable, cash receipts, and related revenue amounts.
- *Workflow Management*: Used to electronically route financial transaction records to designated FFMS users for approval.

Each DHS component that uses FFMS has its own instance of FFMS including separate, partitioned back-end databases. The structure of FFMS limits the information users can access to that of their own component. NPPD has two separate instances of FFMS; one for the Office of Infrastructure Protection, and one for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. NPPD users that support the Federal Protective Service (FPS), which was part of ICE until transferred to NPPD in 2009, also have separate query/read only accounts to access the ICE instance of FFMS to access historical financial transaction data for FPS.

Through reimbursable agreements, ICE provides financial services to the other components that use FFMS. Specifically, ICE processes collections and payments for the other components, and conducts debt collection activities on their behalf. ICE OFM personnel who perform these functions have separate user accounts by which they access the other components' instances of FFMS and record information relevant to the financial services ICE provides. Because ICE is the system owner of FFMS, limited users within the ICE Office of the Chief Information Officer (OCIO) can access the other components' instances of FFMS to provide IT support services (e.g., manage user access, system maintenance and troubleshooting, etc.).

Because the data included in the components' instances of FFMS differs based on each component agency's specific mission and authorities, this PIA will describe the general types of data common to all components in FFMS, such as payroll data, and the additional data that is included in the ICE instance of FFMS. To the extent other component instances of FFMS contain data other than that already described below, that data will be described in an appendix to this PIA added at a later date.

² FACTS I is a system that collects agency pre-closing adjusted trial balances, and FACTS II is a computer program that allows agencies to submit required budgetary information to Treasury. FACTS I and II reflect federal agency budgetary information required for the Report on Budget Execution and Budgetary Resources, the Year-End Closing Statement, and the Program and Financing Schedule of the President's Budget.



ICE Instance of FFMS

The ICE instance of FFMS (FFMS/ICE) is used for the financial transactions described above pertaining to employees, government contractors and vendors, and customers. ICE also conducts financial transactions with individuals or entities that post cash or surety immigration bonds for the release of aliens held in ICE detention. These individuals or entities are known as “obligors.” Using information obtained from another ICE OFM system known as the Bond Management Information System (BMIS), FFMS records immigration bond-related financial transactions, such as interest paid to the obligor and withholding of tax.³ BMIS electronically sends a batch file to FFMS every day containing identifying information about the bond obligors. Using data from BMIS, FFMS records the collections from obligors and ICE’s payments of principal and/or interest once the bond is closed, cancelled, or breached. When processing payments to obligors, ICE personnel at the ICE Burlington Finance Center extract the required information for reporting to Treasury (including the obligor’s name, address, financial data, etc.) from BMIS into a batch data file. This data file is then directly uploaded into the Treasury’s Secure Payment System (SPS)⁴ for transmission to Treasury, which then processes the payment via Electronic Funds Transfer (EFT) or paper check on behalf of ICE. Upon successful transmission of the batch file to Treasury, the same batch file is transmitted to FFMS in order to record the payments. FFMS is also used to report taxable income and send withheld taxes to the Internal Revenue Service (IRS) at Treasury. No information is returned to BMIS from FFMS.

Additionally, with the publication of this PIA, ICE will deploy the Financial Reporting Repository (FRR), which is a business intelligence product used by ICE OCFO as the reporting system for FFMS. In the initial deployment, FRR will ingest selected general ledger and financial transaction information (e.g., transactions, payables and receivables) from FFMS/ICE using a custom extraction, transformation, and loading (ETL) process. The information received from FFMS will contain primarily financial transaction data but also limited PII about DHS employees, contractors/vendors, customers and members of the public participating in certain DHS programs. FRR will also receive reports extracted from the Government Wide Accounting System (GWA)⁵ which contain general ledger information and ICE’s funding balance with Treasury. ICE will use FRR’s reporting capabilities to support OCFO’s internal and external reporting needs (e.g., congressional, senior management and program office, budgetary, etc.).

Contractor/Vendor Commitment, Obligation and Payment Process

As an example, an FFMS user enters a request from a program office to acquire a service or product. The FFMS user will manually create a commitment by entering basic information about the

³ For a description of BMIS (which was previously known as BMIS Web), see the DHS PIA *Bond Management Information System/Web Version (BMIS Web) Interface and Collection* (November 20, 2009).

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_bmisweb_update.pdf.

⁴ SPS is an application used by federal agencies to submit payment schedules to the Treasury for executing payments (i.e., via paper check or EFT) on their behalf.

⁵ GWA supports the central accounting and reporting functions and processes associated with budget execution, accountability, and cash/other asset management. This includes the collection and dissemination of financial management and accounting information from and to federal agencies.



request (e.g., type of service, number or quantity of product) and the requestor (e.g., name, program office, and phone number). The FFMS user also searches and selects the contractor/vendor identified in the request from the vendor table in FFMS, which is a small repository of contractors/vendors that provide services to DHS. Upon selecting the contractor/vendor from the vendor table, information about the contractor/vendor is automatically populated in the commitment including company name, point of contact, address, Data Universal Numbering System (DUNS) number, taxpayer identification number (TIN)⁶, etc. Once the commitment is entered into FFMS, the user submits it to a Funding Certifier for review, and then it is routed to an Approving Official for final approval. After being approved in FFMS, the FFMS user selects the commitment record in order to create an obligation record. Once the services or goods have been provided the vendor sends an invoice to the ICE Burlington Finance Center for payment. A payment technician then creates the payment in the Payment Management module by entering the FFMS document number (assigned during the commitment approval process and creation of the obligation record) of the corresponding obligation record. After the payment record is created and approved, it must be certified by a designated Certifying Official, at which time the payment records are then batched for transmission to Treasury based on the payment type (i.e., EFT or paper check), agency location code and designated Treasury regional finance center. Once batched, a designated data entry operator (DEO) uploads and enters the summary of the scheduled batch data (including confirmation number and dollar amount) into the Secure Payment System (SPS) for review and approval by a Certifying Official. Upon certification of the batch payments, the payments are transmitted electronically within SPS to the Treasury which then returns a confirmation notice of receipt to the agency.

Customers and Collections Process

Financial transactions for customers are typically documented in reimbursable agreements between the customer and the participating DHS component (i.e., ICE, USCIS, S&T, NPPD, OHA, or MGMT), also known as the “servicing agency.” The reimbursable agreement process is initiated when a customer and servicing agency enter into a formal agreement (known as an Inter-Agency Agreement⁷) for goods or services to be provided from the servicing agency to the customer and for the servicing agency to subsequently be reimbursed for the incurred costs by the customer.

Once the reimbursable agreement is established and approved by the customer and servicing agency, the document is forwarded to the ICE Burlington Finance Center for processing. An accounting technician reviews the agreement, and then enters the agreement as an obligation record in the servicing agency’s respective instance of FFMS, which includes establishing the project code, reimbursable agreement record, reimbursable orders, and allocating funds to the reimbursable project. The servicing agency tracks its expenses and costs for providing the goods and services to the customer in the obligation record so that later a bill can be generated. Upon establishing the reimbursable agreement in FFMS, the payment technician notifies the servicing agency that the agreement is available for use. The servicing agency will then commit and/or obligate funds utilizing the project code established by the payment technician, which links the existing obligation and subsequent expenditures to the reimbursable project

⁶ In cases of sole proprietors, the TIN could be the individual’s social security number (SSN) or a vendor’s Employer Identification Number (EIN).

⁷ Specific to FPS, reimbursable agreements are documented in a Security Work Authorization (SWA) agreement.



code and agreement established. Throughout the duration of the agreement, the servicing agency will compile and routinely process (i.e., two times per month) vendor receipts, invoices or other charges to identify and generate a bill to the customer for accumulated expenses incurred by the servicing agency. When generating a bill, an FFMS user reviews the accumulated expenses against the agreement account data to ensure the appropriate project and transaction codes are correct. Once the bill is generated, it is reviewed and approved by an accounting technician and a collection process is initiated. The majority of invoices are collected via the Treasury's Intra-Governmental Payment and Collection (IPAC) system, which facilitates intra-governmental federal e-commerce by transferring funds, with related descriptive data, from one federal agency to another on a real-time basis. The collections are then reconciled in FFMS automatically, and this process continues until completion of the reimbursable agreement.

Member of the Public Payments and Reimbursements Process

Specific to the ICE instance of FFMS, payments for immigration bonds occur when a bond has been cancelled or breached.⁸ When an immigration cash bond is cancelled the principal amount of the bond is returned to the obligor plus any accrued interest, which is calculated based on the bond post date and cancellation date. When an immigration cash bond has been declared breached, only the interest amount is returned to the obligor. All immigration bond payments are calculated in BMIS and transmitted by the ICE Burlington Finance Center to the Treasury via SPS in the same manner described above. Upon successful transmission to Treasury, the same batch data file is transmitted from BMIS to FFMS to record the payments.

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?

Authority for maintenance of FFMS is provided in 8 U.S.C. §§ 1103 and 1226 as well as 8 Code of Federal Regulation (CFR) Part 103. Authority to collect taxpayer identifying number from each person doing business with the agency is provided in 31 U.S.C. § 7701(c).

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

The information in FFMS is collected, used, disseminated and maintained in a manner consistent with the purposes, categories of records, routine uses and retention periods described in the following, government, department-wide and specific DHS component SORNs published in the *Federal Register* and available on the DHS Privacy Office website (www.dhs.gov/privacy):

⁸ An immigration bond is considered "cancelled" when all terms and conditions of the bond are satisfied, but if all terms and conditions are not met (e.g., the alien does not appear for their court hearing) the immigration bond is considered "breached."



- GSA / GOVT – 003: Travel Charge Card Program System of Records (69 FR 4517, January 30, 2004)
- DHS / ALL – 007: Department of Homeland Security Accounts Payable System of Records (73 FR 61880, October 17, 2008)
- DHS / ALL – 008: Department of Homeland Security Accounts Receivable System of Records (73 FR 61885, October 17, 2008)
- DHS / ALL – 019: Department of Homeland Security Payroll, Personnel and Time and Attendance Records (73 FR 63172, October 23, 2008)
- DHS / ICE – 004: Bond Information Management System (74 FR 57891, December 1, 2009)

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

Yes. The system security plan was completed as part of the Certification & Accreditation for FFMS. The Authority to Operate for FFMS was granted on January 19, 2010 and expires in three (3) years.

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

Yes. A retention schedule for records maintained in FFMS was approved by NARA when the system was part of the legacy Immigration and Naturalization Service. ICE is currently in the process of reviewing and updating the records retention schedule for FFMS.

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.

Information contained in FFMS that pertains to DHS employees and contractors/vendors is not subject to the requirements of the PRA.

Information contained in FFMS/ICE that pertains to the posting and reimbursement of immigration bonds (i.e., Form I-352, Immigration Bond) is covered by the PRA, specifically the following information collection: OMB No. 1653-0022.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.



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

FFMS collects, uses, disseminates and maintains information about DHS employees, contractors/vendors, customers and members of the public. Specifically, FFMS contains the following categories of information:

- *Employee personnel information:* Limited to DHS employees, and includes name, address, Social Security number (SSN), occupational data (e.g., job title, duty station, etc.), salary, time and attendance data, health benefit data (e.g., personnel-selected insurance plans and costs), and retirement data.
- *Business-related information:* Limited to contractors/vendors and customers, and includes name of the company/agency, point of contact, telephone number, mailing address, email address, contract number, vendor number (FFMS-generated), DUNS number, and TIN, which could be a SSN in the case of sole proprietors set up as individuals.
- *Financial information:* Includes routing transit number, deposit account number, account type, credit card number, debts (e.g., unpaid bills/invoices, overpayments, etc.), and remittance address.

The following data is also contained in FFMS/ICE:

- *Immigration-related information:* Limited to members of the public applying for immigration benefits, obligors (individuals, entities, or surety companies) posting immigration bonds, and aliens detained by ICE eligible for bond. Such information includes Alien Registration Number (A-Number), obligor name and address, obligor number (FFMS-generated), bond number, total bond and interest amount, bond post date, and bond breach date and number (if applicable).

FFMS also supports external and internal financial-related reporting requirements (e.g., to Treasury for tax and unpaid debt collection purposes). Both routinely and on an *ad hoc* basis, FFMS is used to generate standard financial reports such as for funding balances, obligation and commitment balances, vendor payments, and status of a specific financial transaction. In addition to the inherent capabilities of FFMS, ICE will begin using FRR to generate more executive-level reports for senior management containing similar information as the FFMS standard reports as well as statistical and general processing, workload and performance metrics.

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

The information maintained in FFMS is primarily received from other systems via direct, automated system connections. These source systems include:

- *FedTraveler:* Government-wide travel management system owned by the Government Services Administration (GSA) that is used by federal employees to manage travel



Homeland Security

Privacy Impact Assessment

ICE, Federal Financial Management System (FFMS)
Page 10

authorizations, vouchers and expenditures. On a daily basis, FFMS receives a batch file from FedTraveler containing new and updated travel records for DHS travelers (i.e., DHS employees and invitational speakers) in order to obligate funds for temporary duty and local travel activity as well as pay funds owed to agency employees under approved travel expense reports.

- *National Finance Center (NFC) Payroll System*: Government-wide payroll system owned by the Department of Agriculture that is used to set up federal employee payroll profiles as well as manage payment of salary and benefits. On a bi-weekly basis, FFMS receives a batch file from the NFC Payroll System containing new and updated DHS employee records and time and attendance records.
- *Treasury's Financial Management Service* – A Treasury bureau that operates a suite of financial systems and services that provide limited financial data to FFMS.
 - Secure Payment System (SPS) – On a daily basis, FFMS receives a batch file from SPS containing payment schedule numbers and check numbers for payments (including immigration bond reimbursements) issued on behalf of ICE or one of the other DHS components that uses FFMS.
 - Intra-Governmental Payment and Collection (IPAC) System – On a daily basis, FFMS receives a batch file from IPAC containing payment schedule numbers, amounts, etc. in order to record payments received from other government agencies for services provided by DHS which are made payable to ICE or one of the other DHS components that uses FFMS.

When contractors/vendors do not exist in FFMS's vendor table, payment technicians manually search and gather business-related information about contractors/vendors from the Central Contractor Registration (CCR) database. CCR is a GSA-owned system that tracks data on all contractors who do business with the federal government. All contractors are required to register with CCR in order to contract with the federal government.

FFMS/ICE receives Financial and Immigration-related information about immigration bond obligors from BMIS. ICE uses this information to process bond-related financial transactions (e.g., interest payments, repayment of principal, etc.) as well as support the withholding of taxes and reporting of income to both obligors (e.g., IRS Form 1099 generation) and the IRS. On a daily basis, FFMS/ICE receives a batch file from BMIS containing new records on immigration bonds. Immigration bond payment information is also recorded in FFMS/ICE upon transmission to the Treasury for payment execution on behalf of ICE.



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

Yes. As discussed in Question 2.2, payment technicians manually search the CCR database to gather contractor/vendor information. The CCR database is available for public searching, however payment technicians have privileged access to CCR in order to gather additional contractor/vendor information in CCR that is not made available to the public (e.g., DUNS number, TIN, or information not made public by the vendor). Payment technicians also use CCR to verify the contractor/vendor is in good standing with the federal government. The contractor/vendor information gathered by the payment technicians is then manually entered into the FFMS vendor table, which is a smaller repository of contractors/vendors that provide services to DHS. This information is used when generating payments for services rendered and transmitting required information to the Treasury for tax purposes (e.g., 1099-INT and 1099-MISC forms).

2.4 Discuss how accuracy of the data is ensured.

The information maintained in FFMS is primarily received from other systems (described in Question 2.2). These source systems generally gather the information directly from the individual or entity about whom it pertains, and as such is considered to be highly accurate. In addition, FFMS employs various internal controls and procedures to ensure the accuracy of FFMS data. For instance, the majority of data in FFMS is received through automated system connections; this increases data accuracy by minimizing data entry errors. Before uploading to FFMS, the source data is also automatically evaluated for errors (e.g., formatting, duplicate records, incorrect financial data/codes), and if errors are found, FFMS will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a FFMS user in consultation with the source system or provider. Once reconciled, the record is re-submitted to FFMS as part of the next automated transmission.

Consistent with DHS Management Directive 4300A, FFMS user roles and accesses are established following the separation of roles and duties principle, which inherently creates accuracy checks in FFMS when processing transactions. Basically, no same FFMS user can create and approve a single financial transaction. As described in the Overview, transactions are generated by one FFMS user and then reviewed and approved by another user. With each layer of review and approval, information in FFMS is checked for accuracy purposes, and errors are returned to the originating FFMS user for correction. Furthermore, when making corrections, users validate the information against the source data, which increases the data accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the information

Privacy Risk: FFMS could present a risk of the over-collection of PII.



Mitigation: ICE only collects information in FFMS necessary to appropriately process financial transactions and as required for reporting to Treasury. Information maintained in FFMS is also primarily received via direct, system connections, which minimizes this risk by limiting the information collected to only the information necessary to appropriately process financial transactions and/or comply with reporting requirements as required by law. Additionally, the SSNs maintained in FFMS for DHS employees and contractors/vendors are visible only to those authorized users with an appropriate need to know based on their user access and prescribed, official duties (e.g., system administrators).

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FFMS uses the categories of information identified in Question 2.1 for the following purposes:

- *Employee Uses:* FFMS uses employee personnel information such as name, SSN, grade, salary, etc. to process employee payroll, health benefits (e.g., personnel-selected insurance plans and costs), external training requests, and business travel. When received from the NFC, employee personnel information is used to verify and match employee records.
- *Contractor/Vendor Uses:* FFMS uses business-related information such as company name, address, DUNS number, point of contact, contract number, etc. to generate commitments and obligations. FFMS also uses this information, including the TIN, to submit information about the contractor/vendor to the IRS for tax purposes. In addition, FFMS uses financial information collected from contractors/vendors such as EFT numbers, routing numbers, etc. to generate payments for services rendered.
- *Customer Uses:* FFMS uses business-related and financial information such as company name, address, point of contact, etc. to generate obligations and collections (i.e., bills/invoices) for debts owed to DHS for services provided to customers.

Specific to FFMS/ICE, certain categories of information identified in Question 2.1 are used for the following purpose:

- *Public Uses:* FFMS uses immigration-related information such as alien name, A-Number, bond number, obligor name and address (where applicable) to generate a payment (including reimbursements).. FFMS verifies and matches existing records to information it receives from BMIS regarding cancelled or breached immigration bonds using Immigration-related information (i.e., the bond number). FFMS also uses financial information about aliens and obligors who have posted immigration bonds to process payments and reimbursements (as appropriate).



Lastly, FFMS uses the information to generate routine and *ad hoc* reports described in Question 2.1 above. Such reporting also includes sharing any of the aforementioned categories of information with external agencies, namely Treasury for tax-related and debt collection purposes as required by law.

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. FFMS is not used to conduct electronic searches, queries or analyses to discover or locate predictive patterns or anomalies.

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

Yes. All DHS components that use FFMS have access to their instance of the system with assigned user roles and responsibilities (described below in Question 8.3). FFMS user roles are consistent across all instances. However, as mentioned in the Overview, NPPD users that support FPS also have separate accounts to access the ICE instance of FFMS to access historical financial transaction data for FPS. Additionally, ICE as the owner and service provider of FFMS has the ability to access the other components' instances of FFMS in order to provide financial services to those components (i.e., to process collections and payments) and to provide IT support services.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access to the information maintained in FFMS.

Mitigation: To mitigate this risk, FFMS employs appropriate role-based access controls so only authorized users have access to their component's instance of the system. The access roles are pre-designated by the individuals' position, which ensures users are only granted access to information necessary to perform their official duties. Additionally, all users receive training regarding the proper use of FFMS and rules of behavior prior to being granted access to the system. All FFMS users complete annual mandatory privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.



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

Individuals are not provided notice at the time information is transmitted to FFMS. Rather, individuals providing information that is ultimately transmitted to FFMS are provided notice at the time of the initial collection using Privacy Act Statements that inform the individuals of the authority for and purpose of the collection, the uses for which the information will be shared, and whether providing the information is mandatory or voluntary. Notice is also provided by this PIA as well as the publication of the SORNs identified in Question 1.2.

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

Since information in FFMS is primarily received from other sources, individuals do not have the option to consent to particular uses of their information once transmitted to FFMS. Once collected, their information is used for the purposes described in this PIA and as described in the SORNs identified in Question 1.2.

At the time of collection, however, individuals may decline to provide information, but failure to provide the information may result in the denial or refusal of a benefit and ultimately the failed processing of a financial transaction (e.g., payment, reimbursement, etc.).

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of FFMS and the data it collects and maintains.

Mitigation: This PIA serves as public notice of the existence of FFMS and the data it collects and maintains. Additional notice is also provided by the publication of the SORNs identified in Question 1.2 as well as at the time of initial collection via privacy act statements on forms and public facing systems.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

All information described in Question 2.1 is retained in FFMS. Under the existing retention schedule and in accordance with NARA general records schedules, the information will be maintained for



6 years and 3 months from the date of appropriation or last activity at which time the data will be deleted from FFMS. Retention of the information for this amount of time is necessary in order to apply any additional expenditures, make corrections to payments (i.e., for overpayments) and account balances as appropriate, and for reporting and auditing purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in FFMS is retained for the timeframes outlined in Question 5.1. The information in FFMS will be maintained for six years and three months in order to ensure the financial transaction information is available for audit purposes and/or review after an appropriation has expired.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Yes. ICE shares Business-related and Financial information maintained in FFMS outside of DHS with the Treasury's Financial Management Service to facilitate payment disbursements. Information shared with Treasury's Financial Management Service is transmitted electronically via a direct upload to the Treasury's SPS system. Transmission of data to Treasury via SPS is protected using public key infrastructure (PKI) encryption. The information shared includes the payee's name, address, TIN (where applicable) and bank account information, and is shared at the time the disbursements are submitted to the Treasury for execution. The Treasury uses the information provided to issue federal payments on behalf of DHS in the form of a paper check or EFT transaction.

As required on an annual basis, ICE shares business-related and financial information maintained in FFMS with the IRS to report payments issued to vendors/contractors for services rendered to DHS. Additionally, ICE also shares immigration-related information maintained in FFMS with the IRS when income taxes are withheld from obligor interest payments, and to report on interest payments distributed to obligors (IRS Form 1099). The information shared includes the obligor's name, address, TIN (where applicable) and amounts paid and withheld. This information is shared with the IRS to support the operation of the federal income tax process and in accordance with the Internal Revenue Code and IRS regulations. Information shared with the IRS is sent electronically through an encrypted transmission to an IRS system, the Filing Information Returns Electronically (F.I.R.E.) System, which is an IRS system



used by financial institutions and other entities including DHS to file required tax documents to report payments and withholdings.

ICE is also required to share information pertaining to debts with Treasury pursuant to the Debt Collection Improvement Act of 1996. The information shared could relate to all categories of individuals for whom financial transactions are processed as well as all categories of information maintained in FFMS. The information shared could include name, obligor name (for immigration bond-related debts), address, TIN (where applicable), SSN (in the case of a DHS employee), and debt amount (e.g., unpaid amount, overpayment amount, etc.). ICE prepares batch data files that are sent electronically to the Treasury via an encrypted transmission to the Treasury Cross-Servicing Program and/or Treasury Offset Program for appropriate handling/processing including sending out debt collection letters, establishing repayment agreements, reporting debts to credit bureaus, withholding wages, and other debt collection activities.

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

The sharing described above is compatible with the original purpose for which the information was collected, namely to perform financial management activities in FFMS. All external sharing falls within the scope of published routine uses defined in the SORNs identified in Question 1.2.

The information that is provided to the IRS for interest payment and information reporting is required under federal income tax laws and regulations. In addition, agencies are required to share unpaid debt information for collection purposes under several federal laws, including the Debt Collection Improvement Act of 1996.

6.3 Does the project place limitations on re-dissemination?

Typically there are no limitations on re-dissemination of this information. Any further sharing and re-dissemination of FFMS data is permitted as authorized by the recipient agency's SORN(s) or information sharing policies.

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

ICE uses the payment schedule dates from when batch payment files are transmitted to Treasury via SPS (described in the Overview) to track disclosures of FFMS data (including PII) outside of DHS. Upon successful transmission to Treasury, the same batch data file transmitted to Treasury is also transmitted to FFMS in order to record the payments. By recording the payment schedule date from the batch file, FFMS records the disclosure of the associated records maintained in FFMS.



6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risks associated with this external sharing are the possible improper dissemination or compromise of information maintained in FFMS.

Mitigation: These risks are mitigated by the fact that information maintained in FFMS is shared in a manner consistent with the routine uses prescribed in the SORNs identified in Question 1.2 or as required by law. FFMS information is also safeguarded in accordance with applicable rules and policies including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information being stored. Additionally, information is securely shared via encrypted system connections.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress, which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals may request access to records about them in FFMS by following the procedures outlined in the SORNs identified in Question 1.2. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interest.

In addition to the procedures above, individuals seeking notification of and access to any record contained in the ICE instance of FFMS, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia>). If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0550, Washington, DC 20528.

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

If individuals obtain access to the information in FFMS pursuant to the procedures outlined in the SORNs identified in Question 1.2, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the SORNs identified in Question 1.2. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.



In addition to the procedures above, individuals seeking notification of and access to any record contained in the ICE instance of FFMS, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia>). If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0550, Washington, DC 20528.

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

The procedures for submitting a request to correct information are outlined in the SORNs identified in Question 1.2 and in this PIA in Questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have access to information maintained about them in FFMS or be able to correct their information.

Mitigation: Individuals can request access to information about them through the FOIA process and may also request that their information be corrected.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

FFMS uses database-level auditing to capture information associated with any viewing, creating, updating or deleting of records in the dataset, and the user that performed the activity. FFMS application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification and destruction that would negate its forensic value.

ICE reviews audit trails on a weekly basis or more often if there is indication of system misuse and at random intervals to ensure users are accessing the updating bond records according to their job function and responsibilities. All logon attempts are recorded in the audit log. The FFMS Information System Security Officer (ISSO) reviews login audit trails at least once per week, or in accordance with the System Security Plan. This review includes regular user login activity as well as Data Base Administrator user login activity. FFMS and supporting infrastructure audit logs will be maintained as part of and in accordance with the existing ICE system maintenance policies and procedures.



ICE is also currently in the process of implementing the Audit Log Management (ALM) tool, which is being developed internally by ICE OCIO to further enhance and automate auditing capabilities throughout ICE. The ALM tool is a robust platform for collecting, managing and reviewing audit log data and offers automated response mechanisms for events identified as suspicious. Additionally, access to the audit data gathered by the ALM tool is limited to only those users with an established need to know such as the ISSO. ALM will be used to manage FFMS audit trail information at a future date.

ICE also has a process in place for investigating and responding to suspicious activities on the system. That process includes automated tools to assist the administrators in their monitoring and analysis and reporting. The process is consistently followed. Additional FFMS runs within the DHS network and is protected by DHS network firewalls.

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

All ICE personnel and contractors complete annual mandatory privacy and security training, specifically the Culture of Privacy Awareness and the Information Assurance Awareness Training.

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

Each user account is assigned certain roles with a defined set of privileges to ensure overall system integrity. The FFMS database administrator can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to DHS personnel who have a need to access the system based on their roles in support of financial administration and management operations at DHS. To gain access to FFMS, users must complete the FFMS user training and submit a request for system access to the authorized point of contact in their program office. The roles and privileges assigned to a particular user are predetermined depending on the user's function. The user roles defined below are consistent across all FFMS instances.

- *Originator* – Create and process commitments and obligations in the FFMS Desktop Screens.
- *Funding Certifier* – Review/edit and certify commitments and obligations, and check funding availability in the FFMS Desktop Screens.
- *Approving Official* – Review and approve or deny commitments and obligations in the FFMS Desktop Screens; cannot edit.
- *Payment Technician* – Create and process bills/invoices; create new vendor entries in the FFMS vendor table; create and process reimbursable agreements.
- *Payment Certifier* – Review and approve or deny bills/invoices for payment certification.



- *System Administrator* – Setup, manage, review, edit, and delete user profiles/accounts, in the Database Administrator Management Screens and other maintenance screens.
- *HelpDesk User (i.e., Database Administrator)* – Create user accounts, reset passwords, and perform system troubleshooting (i.e., technical and maintenance modifications) in the various FFMS instances, as necessary.

Specific to FFMS/ICE, because FPS was a part of ICE until 2009 when it transitioned to NPPD, a special user role (other than the roles previously identified) was created for NPPD users to access FFMS/ICE in order to access historical FPS financial transaction data. These NPPD users are assigned unique usernames and passwords, and are provided a general “QRYALL” user profile that allows them query and read only access to FFMS/ICE. Like other FFMS users, these users and their associated activities are monitored and audited as described in Question 8.1.

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?

Component financial program managers coordinate with component Privacy Officers to review and assess new uses of information consistent with DHS established procedures (i.e., using Privacy Threshold Analyses). Where necessary, component Privacy Officers will work with component financial program managers, counsel and the DHS Privacy Office to publish amendments to the SORNs identified in Question 1.2.



Additionally, component financial program managers, component Privacy Officers, and counsel review interconnection service agreement (ISAs) for internal and external systems that interface with FFMS to ensure adequate protections are in place to safeguard information transmitted between systems.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
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