



Privacy Impact Assessment  
for the

# DHS Financial Management Systems

**DHS/ALL/PIA-053**

**July 30, 2015**

**Contact Point**

**Chip Fulghum**

**Chief Financial Officer**

**Department of Homeland Security**

**202-282-8000**

**Reviewing Official**

**Karen L. Neuman**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## Abstract

Department of Homeland Security (DHS) Financial Management Systems (FM Systems) include web-based, workflow management, and financial transaction systems that provide core financial management functions for the Department and are designated by the Chief Financial Officer (CFO) as financial management systems. DHS FM Systems are used to create and maintain records of each allocation, commitment, obligation, travel advance, and accounts receivable issued by the Department. The systems contain personally identifiable information (PII) about DHS employees, contractors/vendors, customers, and members of the public that participate in DHS programs. This privacy impact assessment (PIA) covers multiple financial management systems with similar practices and functional capabilities. This PIA covers all core CFO-designated systems listed herein and in the Appendix. DHS will publish a separate PIA for any system that differs substantially or that raises distinct privacy risks from those covered by this PIA. DHS is conducting this PIA because DHS FM Systems collect and maintain PII.

## Overview

DHS Chief Financial Officer (CFO)-Designated Systems are information technology systems that require additional management accountability to ensure effective internal control exists over financial reporting. CFO-Designated Systems can be non-financial, financial-mixed, or true financial systems;<sup>1</sup> External Information Systems (EIS); or General Support Systems (GSS). Generally, DHS uses its CFO-designated systems 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, 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.

---

<sup>1</sup> A financial system is an information system, comprised of one or more applications, that is used for any of the following: (i) collecting, processing, maintaining, transmitting, and reporting data about financial events; (ii) supporting financial planning or budgeting activities; (iii) accumulating and reporting cost information; or (iv) supporting the preparation of financial statements. A mixed financial system is a system that supports both financial and non-financial functions of an organization.



- *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, or customers who receive goods and services from DHS. For several Components, financial transactions may also occur with members of the public who participate in programs in which 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, trusted traveler programs, or credentials). These transactions are generally conducted via Treasury's Pay.gov system.<sup>2</sup>

### *Criteria for CFO-Designated Systems*

CFO-Designated Systems perform important functions within the financial reporting process at a Component or across the Department. However, not all systems in the Department's inventory will be CFO-Designated. These systems require additional management accountability to ensure effective internal control exists over financial reporting, and must meet a set of criteria to receive the designation.

CFO-Designated Systems are not simply limited to those systems owned by the Department. The Department depends on cross-Component servicing, federal shared service providers, and external commercial providers to perform key financial management functions. In addition, several DHS Components operate as financial management service providers for other DHS Components.

Additionally, the Department uses external federal agencies and commercial service providers to perform key processes. Systems at these entities are considered EIS, and may also be considered CFO-Designated.

CFO-Designated Systems are not limited to applications. The financial transactions and reports generated or processed by CFO-Designated Systems traverse GSS (*i.e.*, networks). National Institute of Standards and Technology (NIST) also requires that GSS have controls in place to protect the transactions from unapproved alteration. DHS 4300A, Attachment R: *Compliance Framework for CFO-Designated Systems*<sup>3</sup> includes network security requirements for protecting data that resides in systems and on the network. These network controls must also be regularly evaluated for design and effectiveness and are frequently included in the scope of security control assessments and audits.

---

<sup>2</sup> See Department of Treasury Pay.gov PIA, available at [http://www.fms.treas.gov/pia/paygov\\_pia%20.pdf](http://www.fms.treas.gov/pia/paygov_pia%20.pdf).

<sup>3</sup> See DHS SENSITIVE SYSTEMS HANDBOOK 4300A, Attachment R (July 24, 2012), available at <https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-R-Compliance-Framework-for-CFO-Designated-Systems.pdf>.



A *CFO-Designated System* can be a:

1. DHS-owned non-financial, financial mixed, or true financial system<sup>4</sup> that is hosted and used within the same Component;
2. Intra-Department EIS that is hosted at one Component and used across the Department;
3. EIS that is hosted at another federal agency or commercial service provider and used across the Department; or
4. GSS (network), supporting applications that sustain key business processes. A GSS normally includes hardware, software, information, applications, communications, data, and users. Examples of a GSS at DHS include a local area network (LAN) with financial applications, a Component or Department-wide backbone, a communications network, or a Departmental data processing center including its operating system and utilities.<sup>5</sup>

Uniform criteria are necessary to ensure that CFO-System designations are made consistently. The most prominent criteria are typically the annual volume of dollars and transactions processed by the system. However, other qualitative factors should be equally considered, such as key interfaces, placement of the system within the financial reporting process, and mission criticality of the system. The following criteria apply to vetting a system and GSS for CFO system designation. CFO-Designated Systems are classified as such when they meet one or more of the criteria in their respective category below.

### *DHS CFO-Designated Systems*

DHS CFO has designated six information technology systems as FM Systems for the Department's core financial management requirements. They include:

- Federal Financial Management System (FFMS) owned and operated by ICE. Services ICE, MGMT, USCIS, NPPD, S&T;
- Financial Accounting and Budgeting System (FABS) owned and operated by FLETC. Services FLETC, I&A, and OPS;

---

<sup>4</sup> A financial system is an information system, comprised of one or more applications, that is used for any of the following: (i) collecting, processing, maintaining, transmitting, and reporting data about financial events; (ii) supporting financial planning or budgeting activities; (iii) accumulating and reporting cost information; or (iv) supporting the preparation of financial statements. A mixed financial system is a system that supports both financial and non-financial functions of an organization.

<sup>5</sup> A general rule of thumb is that if systems residing on a GSS are considered CFO-Designated, the GSS will likely be deemed CFO-Designated as well. However, this is not always the case. Together, the system and GSS provide protection and security over the financial data. DHS 4300A, Attachment R, details control requirements for CFO-Designated systems, and includes specific requirements for specific GSS (network layer) level controls. For example, the Access Control (AC) and Configuration Management (CM) sections of Attachment R require specific network and communications security controls from DHS 4300A, Section 5.4.



- Core Accounting System (CAS) Suite owned and operated by USCG. Services USCG, TSA, and DNDO;
- Travel Manager, Oracle Financials, Compusearch/Purchase Request Information System (PRISM), and Sunflower (TOPS) – USSS;
- Systems, Applications, and Products in Data Processing (SAP) – CBP; and
- Web Integrated Financial Management Information System – FEMA.

DHS FM Systems are a collation of existing independent systems used to create and maintain records of each allocation commitment, obligation, travel advance, and accounts receivable issued by the Department. DHS also has smaller financial management systems and applications that are CFO-designated but not considered “core” financial management systems. These systems are described in the Appendix to this PIA. DHS will publish a separate PIA for any system that differs substantially, or that raises distinct privacy risks from those covered by this PIA. If DHS designates other systems as FM Systems, DHS will update this PIA or Appendix as appropriate.

### 1. Federal Financial Management System (FFMS) - ICE

U.S. Immigration and Customs Enforcement’s (ICE) Office of the Chief Financial Officer (OCFO), Office of Financial Management (OFM) is responsible for operating and maintaining FFMS, which supports and processes financial management activities for ICE and five other DHS Components, Directorates, or Offices (“Components,” for purposes of this PIA) specifically, United States Citizenship and Immigration Services (USCIS), Office of Science and Technology (S&T), the National Protection and Programs Directorate (NPPD), Office of Health Affairs (OHA), and Office of Management (MGMT)<sup>6</sup>. 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) 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;

---

<sup>6</sup> For the purpose of this discussion regarding financial management systems, references to MGMT include the Office of the Secretary and Executive Management (OSEM) [*i.e.*, the Offices of Policy, Privacy, Civil Rights and Civil Liberties, Legislative Affairs, Public Affairs, General Counsel].



- 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 (OMB)) 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.<sup>7</sup> This module enables a user to track allocation costs (*e.g.*, labor, expenses, hours).
- *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 that detail current expenditures, allocations, collections, and payments for reporting to DHS (*e.g.*, CFO Reports) and Treasury (*e.g.*, Federal Agencies' Centralized Trial-Balance System [FACTS] I and II Reports).<sup>8</sup> 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 Treasury; and recording financial transactions to update the general ledger with the proper accounts payable and related expense amounts.

---

<sup>7</sup> 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.

<sup>8</sup> 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.



- *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 separate instances of FFMS; one for the Office of Infrastructure Protection and one for the Office of Biometric Identity Management (OBIM). 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. FPS still uses the ICE instance.

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, troubleshooting).

## **2. Financial Accounting and Budgeting System (FABS) – FLETC**

The FABS application is an all-in-one financial processing system.<sup>9</sup> It functions as the automated accounting and budgeting system for the Federal Law Enforcement Training Center (FLETC). FLETC uses FABS to support its financial management and fixed asset management system requirements. This version of the software requires a separate contract to provide custom and technical support. This software provides a web based architecture that supports: a web user interface; an open-standards-based interface for integration with external systems; and service-oriented capabilities. It also provides reporting capabilities, data management capabilities, and business rule capabilities.

As an Internal Shared Service Provider (ISSP) for the Department of Homeland Security, FLETC currently provides financial management services to the Office of Intelligence and Analysis (I&A) and the Office of Operations Coordination and Planning (OPS). FLETC currently

---

<sup>9</sup> FLETC "Momentum" IT system functions as the single computerized accounting and budgeting system for FLETC. Momentum resides within the security accreditation boundary of FABS.



processes approximately 1,000,000 General Ledger (GL) transactions annually. These transactions consist of the following document types: vendor payments, vendor records, payroll documents, credit card purchases, travel, cash receipts, and dunning as well as approximately 30,000 reports.

### 3. Core Accounting System (CAS) Suite – USCG

The United States Coast Guard (USCG) CAS Suite<sup>10</sup> provides integrated accounting, financial reporting, and asset management services to USCG, the Transportation Security Administration (TSA), and the Domestic Nuclear Detection Office (DNDO). The CAS Suite consists of six main subcomponents including: Core Accounting System (CAS), Financial Procurement Desktop (FPD), Workflow Imaging Network System (WINS), Sunflower, Pay and Personnel Center (PPC) Checkfree, and the Contract Information Management System (CIMS). The CAS Suite provides a wide variety of business functions as described below.

#### *Core Accounting System*

The CAS Suite has been the primary Financial Management Solution (FMS) for USCG, TSA, and DNDO. However, the Components now have a need to move this capability to a new FMS solution provided by a Federal Shared Service Provider (FSSP). To address this common need, each Component established its own acquisition project under the DHS Financial Systems Modernization (FSM) Initiative.

- DNDO - Financial, Acquisition, and Asset Management Solution (FAAMS)
- TSA - Financial Services Replacement (FSR)
- USCG - Financial Management Service Improvement Initiative (FMSII)

The goal of the three referenced DHS projects is to transition from the legacy CAS solution to a common shared FMS solution. DNDO, TSA, and USCG intend to transition to the Oracle Federal Financials (OFF), hosted by the Department of the Interior-Interior Business Center (DOI-IBC), which is a FSSP. Under this approach USCG, DNDO and TSA will not own, design, configure, manage, host, or customize financial management software and associated hardware. Instead, DOI-IBC will be responsible for providing the required FMS functionality as a service and deliver Component requirements through configuration of the Commercial-Off-The-Shelf (COTS) solution to the maximum extent possible, while maintaining alignment with Treasury Department's Office of Financial Innovation and Transformation (FIT) modernization evaluation criteria for financial services.

All key CAS Suite data and functionality referenced in the earlier section of this document will be delivered through the new DHS FSM service. All applications within the new service will

---

<sup>10</sup> See DHS/USCG/PIA-009 Core Accounting Suite (September 18, 2009), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_uscg\\_cas.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_cas.pdf) for additional information. However, note that in 2017 CAS Suite will be replaced by the Financial Management Service Improvement Initiative (FMSII). USCG will retire the CAS PIA and replace it with a new PIA for FMSII prior to deployment.



be web accessible to the end users via an interface provided by DOI-IBC.

Of the three DHS Components planning to transition into this new service, DNDO will be the first to transition (FY16), followed by TSA (FY17) and USCG (FY18) respectively. To ensure successful transitions, multiple tests, involving data transfer (which will include PII data) from CAS to the new solution, are currently being conducted by the FSSP, with additional tests scheduled in FY15, FY16 and FY17 respectively. Following USCG's successful migration over to the new FSM service, CAS will be dispositioned.

The personally identifiable information (PII) that passes through the Core Accounting System is required in order to process financial data. The Core Accounting System services a user base of military personnel, civilian employees, and contractors from USCG, DNDO, and TSA. The functions of the Core Accounting System include:

- Processing and payment of obligations to commercial and government vendors and members;
- Collection of payments received for services from the general public, contractors, or other government agencies;
- The ability to track, report costs, and receipts on projects;
- Maintenance of a general ledger containing the financial status of each agency serviced in terms of planned versus actual expenditures, obligations, accruals, and commitments for industrial projects; and
- Asset management including the ability to track the original cost, the current value, owner, and location of all capital assets and inventory.

#### *Finance and Procurement Desktop (FPD)*

FPD is the enterprise-wide system used by USCG, TSA, and DNDO to create and manage simplified procurement documents and to maintain accurate accounting records agency wide. Some functions of FPD include:

- Ledger management;
- Budgeting and funds distribution;
- Procurement (procurement requests and simplified acquisitions);
- Receipt of goods/services (accruals);
- Interoperability with the USCG Core Accounting System;
- System administration (account management & setup);
- Reconciliation; and



- Reports.

FPD is designed to meet the needs of the user community by providing a simplified view of both funds spent and funds available, in essence acting as an electronic checkbook for funds management. Purchase Orders are created in FPD and then transmitted and captured by the Core Accounting System. After the process is complete, a reconciliation occurs that is similar to how an electronic checkbook balances its accounts with a statement from a bank. With this functionality, as well as the application's ease of use, FPD is similar to leading commercial checkbook programs. The difference between these products and FPD is that FPD incorporates all of the federal government accounting and procurement practices to meet the needs of federal agency end-users.

The FPD portal uses graphical user interface (GUI) screens for the Web. Real-time integration also exists among FPD, Contract Management Information System, and Core Accounting System. Integration allows financial events from FPD to be recorded immediately in the Core Accounting System. FPD's integration capabilities result from the use of Web-friendly technologies.

### *Workflow Information Network System (WINS)*

WINS is the USCG imaging and document processing system. Paper documents (purchase orders, obligations, modifications, receiving reports, invoices, correspondence, etc.) are electronically loaded or scanned directly into the system upon receipt. For paper documents and fax images received, relevant data elements are entered into the system and associated with the document image in WINS. Files received electronically are entered into the system and images are rendered automatically. All documents entering the system are routed, or "workflowed," to the appropriate accounting operations team at the Financial Crimes Enforcement Network (FINCEN) for processing.

WINS allows electronic images of paper documents to be processed according to procedures established at FINCEN. Processing procedures allow for data verification, reconciliation, and prompt payment of invoices. User roles and workflows established within WINS ensure established business practices are followed while the separation of accounting duties is maintained. Information flows to several information systems that are dependent on WINS, but are external to the application. WINS functions include:

- Producing accurate and timely financial management information and related business reports;
- Processing financial transactions effectively;
- Executing fiduciary and stewardship responsibilities consistent with policy and regulatory authorities; and



- Establishing and maintaining accounting controls over Coast Guard resources.

### *Contract Management Information System (CIMS)*

CIMS is a contracting management system that is used for formal contract creation and management, including milestone planning, solicitations, award, and closeout. This system is integrated with FPD to receive commitments and send contract procurement information back to FPD. The primary users of the system include the contracting officer and contracting specialists. CIMS functions include:

- Creation and management of milestones, solicitations, multiple award setup, and formal contract acquisitions;
- Integration with FPD to receive commitments and send contracts back to FPD;
- Combination of Purchase Request Information System (PRISM) and a customized interface to FPD.

### *Sunflower Asset Management (SAM) Subsystem*

SAM is a property management system providing primary business functions such as acquisitions, transfers, retirements, modifications, and asset tracking. SAM is integrated with Oracle Financials Fixed Assets (FA) for capitalized asset transactions.

Although the USCG uses the Oracle Financials FA module to manage assets and perform property management, Sunflower is hosted by FINCEN for use by TSA. Sunflower is fully integrated with the Oracle Financials FA module for capitalized asset transactions; however, it is not considered to be a module of Oracle Financials because it was developed by a third party. Sunflower does not reside in the same Oracle instance as the Core Accounting System. TSA uses SAM as the property management system of record. SAM functions include:

- Property management system, which provides the primary business functions like Acquisitions, Transfers, Retirements, Modifications and Asset tracking;
- Integrated with Oracle Financials Fixed Assets for capitalized asset transactions;
- FPD is integrated with Sunflower by providing the purchase order and/or receipts to create assets;
- PPC Checkfree Subsystem; and
- Supports the reconciliation of military payroll with four reconciliation sets and a single general ledger.

#### **4. TOPS – U.S. Secret Service (USSS)**

TOPS is an Enterprise Financial Management System that consists of the Travel Manager, Oracle Financials, Compusearch/PRISM, and Sunflower (TOPS) components that support the



acquisition, accounting, travel, and property management functions of the USSS. These components comprise a single, comprehensive, integrated financial management system. TOPS is used by the entire USSS, including field offices.

### **5. Systems, Applications and Products in Data Processing (SAP) – U.S. Customs and Border Protection (CBP)**

The CBP SAP Program is a major integrated financial information system using a commercially available software product, SAP, on a dedicated client server platform. CBP implemented SAP to:

- Combine many old system functions into one more efficient system;
- Eliminate old legacy systems with insufficient security controls;
- Support management goals of the CBP Office of Administration by aligning and improving two core processes: asset (*e.g.*, budget, logistics, procurement, property, and related policy) and revenue (*e.g.*, accounting and commercial operations: trade, tariff, and law enforcement);
- Provide an integrated solution to allow the agency to process and interpret financial data more effectively;
- Develop an agency-wide control and integration system for financial information, which is essential to strategic decision-making;
- Incorporate tools included in the public sector, solution management, and travel management extension sets, to enhance customer service; and
- Facilitate a shift in the role of finance from a transaction process/recordkeeping function to a more analytical and decision making function.

SAP is based on client-server architecture and is accessible throughout CBP. SAP uses a relational database (Oracle) to track information, and allows users to provide finance, procurement, property, and logistic support for all of CBP. SAP is an Enterprise Resource Planning (ERP) System, which provides an integrated, enterprise-wide information software solution.

SAP consists of modules. Each module provides a unique functionality for a specific business process. Since SAP is an integrated system, all modules interact with each other to share information. Information is only entered once into SAP, and the same information can be accessed from other modules. CBP implemented the following modules:

- Accounts Payable (AP): Allows CBP the ability to generate and uniquely identify multiple types of payments with unique formats.
- Asset Accounting (AA): Tracks all CBP personal properties including custom-owned real property assets and capital/leasehold improvements along with depreciation.



- **Budget Control System (BCS):** Provides flexible data entry options (Transaction codes, screen variants, user defaults, GUI, etc.), Multi-level funds check, and ability to route messages when budget is exhausted. It has the capability to drill down to the spending source document.
- **Business Information Warehouse (BW):** Allows for one fully integrated reporting system with real-time query and reporting capabilities.
- **Controlling (CO):** Tracks costs by Cost Centers and Internal Orders.
- **Financial Accounting (FI):** Acts essentially as the regulatory ‘books of record,’ including Funds Management, Accounts Payable, Accounts Receivable, General Ledger and closing.
- **General Ledger (GL):** Provides all details to support GL balances.
- **Special Purpose Ledger (SPL):** Provides the capability of Special Ledger and Split Processor to capture data for specialized agency reporting.
- **Funds Management (FM):** Generates details to support end user budget monitoring and GL balances.
- **Human Resources (HR):** Creates organizational structure and personnel administration for support of other modules (Note: Does not replace systems used by Human Resources Management (HRM)).
- **Materials Management (MM):** Standardizes all procurement processes.
- **Public Budget Formulation (PBF):** Provides a collaborative environment to accommodate the requirements of the end-to-end public sector budget formulation process.
- **Profitability and Cost Management (PCM):** Supports modeling business according to the activities that it carries out using Activity Based Costing (ABC).
- **Plant Maintenance (PM):** Manages and tracks maintenance requirements for CBP real and personal properties and includes corrective and preventative maintenance.
- **Procurement for Public Sector (PPS):** Facilitates the development and execution of the contracting process.
- **Project Systems (PS):** Tracks project costs, activities, tasks, and milestones.
- **Real Estate (RE):** Tracks all CBP-occupied and managed facilities.
- **Reimbursable Agreements (RIA):** Includes Internal Orders and Sales & Distribution.
- **Standard reporting from all SAP Modules:** Allows flexible report creation options.
- **Travel Management (TM):** Provides all details to support Travel Management.



- Workflow (WF): Routes documents for approval, information, and action.

As an integrated ERP, SAP processes transactions in real time. Data is entered once, which reduces the scope for error and results in a single source of reliable data. SAP establishes budget and performance integration as a core capability of the information management system. Electronically linking automated business processes including requisitioning, receiving, invoicing, payment processing, and accounting allows CBP to be more efficient because costs can be captured once.

The drill-down capability of SAP is a powerful tool that allows users to see the details of original documents. For example: from a SAP procurement invoice, users can drill down to the goods receipt and acceptance, purchase order, and purchase requisition. Once the business process is complete, links also allow CBP users to go from the purchase requisition to the purchase order, goods receipt and acceptance, and invoice.

## **6. Web Integrated Financial Management Information System (Web-IFMIS) – Federal Emergency Management Agency (FEMA)**

FEMA Web-IFMIS is FEMA's official accounting and financial management system that tracks all of FEMA's financial transactions.<sup>11</sup> Web-IFMIS does not collect information directly from individuals; the information contained in the system is pulled from other systems. Web-IFMIS provides FEMA's financial managers a global view of all FEMA's financial systems. Web-IFMIS uses information provided through these various subsystems in order to make payments to entitled groups (grantees), FEMA employees for payroll and travel reimbursement, and contractors and other vendors for payment of services. Web-IFMIS is also used to account for the expenditure of public funds as mandated under various statutes, Executive Orders, OMB guidance, regulations, and DHS and FEMA policies. To account for expenditures, Web-IFMIS generates report invoices, payment receipts, cash receipts, commitments, obligations, receiving reports, expenditures, and advanced charges.

Web-IFMIS carries out the budgeting, management of vendor accounts, payment approval, and accounting for FEMA's finances. The process begins when Congress appropriates and OMB approves FEMA's funding. Next, FEMA's OCFO establishes accounts within Web-IFMIS to correspond with the funding appropriated by Congress and approved by OMB. FEMA program offices then request allocation of funds, via Web-IFMIS's subsystems, as part of FEMA's annual and ongoing budgeting, financial, and accounting processes.

FEMA's OCFO receives funding requests from the various program offices and processes these requests by first reviewing the request and determining whether funds are available for the transaction. If funds are available then FEMA commits the funds in Web-IFMIS to prevent those funds from being used for any other purpose. FEMA's OCFO also reviews the requests to make

---

<sup>11</sup> For additional FEMA-specific information about Web-IFMIS, please see DHS/FEMA/PIA-020(a) Web Integrated Financial Management Information System (Web-IFMIS) (August 16, 2013), available at <http://www.dhs.gov/privacy-documents-fema>.



sure that vendor accounts are established for each individual, entitled group, or entity identified on the requests. FEMA establishes vendor accounts using PII, including name and a unique identifier (e.g., Social Security number (SSN), employer identification number). Once funding is appropriated and committed and the proper vendor accounts are established, FEMA is able to process payments or provide reimbursements to those individuals, entitled groups, or entities referenced on the initial requests.

## 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 DHS FM Systems 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).

- The Chief Financial Officers Act of 1990<sup>12</sup> – Requires agencies to both establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting.
- Federal Financial Management Improvement Act (FFMIA) of 1996<sup>13</sup> – Requires federal financial management systems to provide accurate, reliable, and timely financial management information to the government’s managers.
- Federal Information Security Management Act (FISMA)<sup>14</sup> – Requires agencies to provide information security controls that are commensurate with the risk and potential harm of not having those controls in place. The heads of agencies are required to annually report on the effectiveness of the agencies’ security programs. “Significant deficiencies” found under FISMA must also be reported as material weaknesses under FFMIA or as a lack of substantial compliance under FFMIA if related to financial management systems.
- OMB Circular A-123 Management’s Responsibility for Internal Control<sup>15</sup> – Defines Management’s responsibility for internal control in federal agencies. Circular A-123 and the statute it implements, the Federal Managers’ Financial Integrity Act of 1982,<sup>16</sup> are at the center of the existing federal requirements to improve internal control. It further provides guidance to federal managers on improving the accountability and effectiveness

---

<sup>12</sup> Pub. L. 101-576.

<sup>13</sup> Pub. L. 104-208.

<sup>14</sup> Pub. L. No. 107-296, *as amended* by Pub. L. No. 108-177.

<sup>15</sup> OMB Circular A-123 (December 21, 2004), *available at* [https://www.whitehouse.gov/omb/circulars\\_a123\\_rev](https://www.whitehouse.gov/omb/circulars_a123_rev).

<sup>16</sup> 31 U.S.C. § 3512.



of federal programs and operations by establishing, assessing, correcting, and reporting on internal control.

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

The information in DHS FM Systems 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](http://www.dhs.gov/privacy)):

- GSA/GOVT-003 Travel Charge Card Program System of Records;<sup>17</sup>
- DHS/ALL-007 Department of Homeland Security Accounts Payable System of Records;<sup>18</sup>
- DHS/ALL-008 Department of Homeland Security Accounts Receivable System of Records;<sup>19</sup>
- DHS/ALL-010 Department of Homeland Security Asset Management Records;<sup>20</sup>
- DHS/ALL-019 Department of Homeland Security Payroll, Personnel and Time and Attendance Records;<sup>21</sup> and
- DHS/ICE-004 Bond Information Management System.<sup>22</sup>

In addition, DHS and three of its Components (DNDO, TSA, and USCG), have signed an interagency agreement with the Department of the Interior-Interior Business Center (IBC) to be the federal shared service provider for the replacement CAS Suite. DOI is currently scheduled to update its SORN, to include USCG, DNDO, and TSA data, before the scheduled DNDO transition date.

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

Yes. Each of the six DHS FM Systems listed above has its own unique system security plan. Each has been granted an Authority to Operate for three (3) years.

---

<sup>17</sup> GSA/GOVT-003 Travel Charge Card Program System of Records, 69 FR 4517 (January 30, 2004).

<sup>18</sup> DHS/ALL-007 Department of Homeland Security Accounts Payable System of Records, 73 FR 61880 (October 17, 2008).

<sup>19</sup> DHS/ALL-008 Department of Homeland Security Accounts Receivable System of Records, 73 FR 61885 (October 17, 2008).

<sup>20</sup> DHS/ALL-010 Department of Homeland Security Asset Management Records, 73 FR 63181 (October 23, 2008).

<sup>21</sup> DHS/ALL-019 Department of Homeland Security Payroll, Personnel and Time and Attendance Records, 73 FR 63172 (October 23, 2008).

<sup>22</sup> DHS/ICE-004 Bond Information Management System, 74 FR 57891 (December 1, 2009).



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

Yes. Records retained by DHS FM Systems are covered by the following retention periods:

Financial Transaction Records: DHS retains financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting for six years after final payment or cancellation, unless longer retention is needed for business use, in accordance with National Archives and Records Administration General Records Schedule 1.1, item 010.

Asset Management Information: Records used to track all DHS-owned or controlled property that has been issued to current and former DHS employees and contractors. Asset management records are destroyed in accordance with the following: National Archives Records Administration General Record Schedule 1.1, item 030, Property, plant and equipment (PP&E) and other asset accounting (two years after asset is disposed of and/or removed from agency financial statement); National Archives Records Administration General Record Schedule 1.1, item 040 Cost Accounting for stores, inventory, and materials (three years); and General Records Schedule 23, Records Common to Most Offices within Agencies (two years).

## **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 DHS FM Systems that pertains to DHS employees and contractors/vendors is not subject to the requirements of the Paperwork Reduction Act (PRA) because the information is not collected directly from the public. DHS FM Systems obtain the information from various underlying component systems, some of which are covered by the PRA.

## **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.**

DHS FM Systems collect, use, disseminate, and maintain information about DHS employees, contractors/vendors, customers, and members of the public. Specifically, DHS FM Systems contains the following categories of information:



- *Employee personnel information:* Limited to DHS employees, and includes name, address, SSN, occupational data (e.g., job title, duty station), 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 Taxpayer Identification Number (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), 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.

DHS FM Systems 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, DHS FM Systems are used to generate standard financial reports such as for funding balances, obligation and commitment balances, vendor payments, and status of a specific financial transaction.

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

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

- *Concur Government Edition (CGE):* Government-wide travel management system owned by the General Services Administration (GSA) that is used by federal employees to manage travel authorizations, vouchers, and expenditures.<sup>23</sup> On a daily basis, DHS FM Systems receive a batch file from CGE containing new and updated travel records for DHS travelers (i.e., DHS employees and invitational speakers) in order to obligate funds for temporary

---

<sup>23</sup> Concur Government Edition (CGE) replaced the former government travel system known as “FedTraveler.” CGE may also be referred to as Enterprise Travel Systems (ETS2).



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 United States Department of Agriculture (USDA) that is used to set up federal employee payroll profiles as well as manage payment of salary and benefits. On a bi-weekly basis, DHS FM Systems receive 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 DHS FM Systems.
  - Secure Payment System (SPS) – On a daily basis, DHS FM Systems receive a batch file from SPS containing payment schedule numbers and check numbers for payments issued on behalf of DHS.
  - Intra-Governmental Payment and Collection (IPAC) System – On a daily basis, DHS FM Systems receive 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 that are made payable to DHS.

When contractors/vendors do not exist in DHS FM Systems 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 that do business with the Federal Government. All contractors are required to register with CCR in order to contract with the Federal Government.

### **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 the public to search; 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 a DHS FM Systems vendor table, which is a smaller repository of contractors/vendors that provide services to DHS and Components. This information is used when generating payments for services rendered and transmitting required information to 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 DHS FM Systems 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 accurate. In addition, each DHS FM System employs various internal controls and procedures to ensure the data accuracy. For instance, the majority of data in DHS FM Systems is received through automated system connections; this increases data accuracy by minimizing data entry errors. Before uploading to a DHS FM System, the source data is also automatically evaluated for errors (e.g., formatting, duplicate records, incorrect financial data/codes), and if errors are found, the DHS FM System will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a user in consultation with the source system or provider. Once reconciled, the record is re-submitted to the DHS FM System as part of the next automated transmission.

Consistent with DHS Management Directive 4300A, DHS FM Systems user roles and accesses are established following the separation of roles and duties principle, which inherently creates accuracy checks in the individual DHS FM Systems when processing transactions. Each DHS FM System employs user roles and access controls that ensure no one user can create and approve a single financial transaction. Transactions are generated by one user and then reviewed and approved by another user. With each layer of review and approval, information in each DHS FM System is checked for accuracy purposes, and errors are returned to the originating 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**: There is a risk of the over-collection of PII.

**Mitigation**: DHS only collects information in its FM Systems necessary to process financial transactions and required for reporting to the U.S. Department of the Treasury. Information maintained in DHS FM Systems is also primarily received via direct system connections, which limits the information collected to only the information necessary to appropriately process financial transactions or comply with reporting requirements as required by law. This risk of over-collection is also not mitigated because of the need to preserve distinct component financial systems as independent enclaves.



## 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.

DHS FM Systems have similar uses of information. DHS FM Systems use the categories of information identified in Question 2.1 for the following purposes:

- *Employee Uses:* DHS FM Systems use employee personnel information such as name, SSN, grade, and salary to process employee payroll, health benefits, external training requests, business travel, and asset management. When received from the NFC, employee personnel information is used to verify and match employee records.
- *Contractor/Vendor Uses:* DHS FM Systems use business-related information such as company name, address, DUNS number, point of contact, and contract number to generate commitments and obligations. DHS FM Systems also use this information, including the TIN, to submit information about the contractor/vendor to the IRS for tax purposes. In addition, DHS FM Systems use financial information collected from contractors/vendors such as electronic funds transfer (EFT) numbers and routing numbers to generate payments for services rendered.
- *Customer Uses:* DHS FM Systems use business-related and financial information such as company name, address, and point of contact 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, and obligor name and address (when applicable) to generate a payment (including reimbursements). FFMS verifies and matches existing records to information it receives from the Bond Management Information System 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).

#### *Reporting*

Lastly, DHS FM Systems use 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.



For example, information from CBP's SAP provides reports that are used for analysis and decision-making. SAP reports significantly reduce the amount of time currently spent on research. From within SAP, Business Warehouse (BW) systems are used as standard reporting solutions that integrate widespread financial data across CBP. Business Warehouse systems are designed for better data visibility across CBP to support accurate and consistent reporting. Report data can be downloaded into local files in formats such as Excel and users have flexibility in the display features using various layouts.

### *Field Offices*

DHS FM Systems users may also transmit financial files (invoices) to field offices. The transactions are recorded in DHS FM Systems. However, most field office system interfaces are not a real-time direct interface with their corresponding DHS FM Systems. Therefore the field offices must execute a data transfer to a specified account and location on the DHS FM Systems to return the processed financial data. DHS financial management personnel then manually rename the file(s) and move it to another file folder where it is processed via a series of batch jobs that are each manually initiated within the corresponding DHS FM Systems application. Finally, each DHS FM System creates a file that is uploaded into the Treasury Information Executive Repository (TIER) system that is located at DHS Headquarters and managed by DHS.

### **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.

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

Yes. All DHS Components that use DHS FM Systems have access to the discrete functionality that supports their Component system with assigned user roles and responsibilities (described below in Question 8.3). DHS FM Systems user roles are similar across all systems; however, DHS FM Systems follow the DHS policy requirements of "least privilege."

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a risk that data may become outdated or incorrect without real-time refresh from all source systems, because of the interconnectedness of DHS FM Systems to multiple external and internal systems.

**Mitigation:** This risk is only partially mitigated. Most DHS FM Systems rely on a data feed from the USDA NFC that is only run once every two weeks. DHS FM Systems vary in their



refresh or update periods; however, all of them refresh at least as often as the NFC feed from USDA.

**Privacy Risk:** There is a risk that DHS FM Systems users export reports to their localized computer terminals.

**Mitigation:** This risk is managed by limiting access to DHS FM Systems to only DHS employees with a financial management business function, and then only to those systems that support their respective component.

**Privacy Risk:** There is a risk of unauthorized use of the information maintained in DHS FM Systems.

**Mitigation:** To mitigate this risk, all DHS FM Systems employ appropriate role-based access control 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 DHS FM Systems and rules of behavior prior to being granted access to the system. All DHS FM Systems users complete annual mandatory privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems.

**Privacy Risk:** There is a risk involving data quality and minimization arising from DHS FM Systems user's practice of manually transmitting financial data to field offices.

**Mitigation:** This risk is only partially mitigated. Ideally, DHS FM Systems should provide methods for incorporating financial management data from DHS field offices into the DHS FM Systems instances as opposed to using Excel or other ad hoc reporting mechanisms. Since the data does not leave the DHS internal network and is shared via email, the financial management data submitted to DHS FM Systems from field offices remains secure.

## 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.**

DHS FM Systems do not generally collect information directly from individuals. Rather, they serve as aggregate financial management systems for transactions from multiple source systems—systems that collect directly from individuals. Individuals providing information that is ultimately transmitted to DHS FM Systems are provided notice at the time of the initial collection by Privacy Act Statements that inform the individuals of the authority for and purpose of the



collection, the uses of the information, and whether providing the information is mandatory. 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 DHS FM Systems is primarily received from other sources, individuals do not have the option to consent to particular uses of their information once transmitted to the DHS FM System. Once collected, their information is used for the purposes described in this PIA and 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, including the failed processing of a financial transaction (*e.g.*, payment, reimbursement).

## **4.3 Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** There is a risk that individuals will not be aware that DHS FM Systems collects and uses their information.

**Mitigation:** This PIA provides notice that the DHS FM Systems use data from other DHS systems. Additional notice is also provided by the publication of the SORNs identified in Question 1.2 as well as by Privacy Act statements at the time of initial collection.

## **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 DHS FM Systems. Under the existing retention schedule and in accordance with NARA general records schedules, the information will be maintained for 6 years from the date of the final payment or cancellation and then deleted from DHS FM Systems. 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, 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 on individual DHS employee computer terminals longer than necessary to accomplish the purpose for which the information was originally collected, inconsistent with the requisite records retention schedules.

**Mitigation:** This risk is not mitigated. All DHS FM Systems incorporate functionality to allow users to export reports and files directly to their local computer terminals. DHS reminds



DHS FM System users through policy and training that they must follow the applicable retention schedules for financial information, regardless of where it is stored.

## 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), how the information is accessed and how it is to be used.**

Yes. DHS shares information maintained in its DHS FM Systems outside of DHS with the below external organizations as explained below. External organizations are responsible for following their own applicable records retention schedules.

#### *Typical External Sharing Transaction*

On a monthly basis, an accountant runs a batch process on a DHS FM Systems Production Server that creates a file. This file is then uploaded manually to the TIER website. DHS uses data to prepare monthly and year-end financial statements for the Performance and Accountability Report (PAR). TIER is a Treasury financial data repository, which collects, processes, and stores summary financial data that is used to produce Treasury's consolidated financial statements required by OMB. The information is provided as an electronic file.

#### Department of the Treasury

DHS FM Systems share information with the United States Department of 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 Treasury's SPS system. Transmission of data to Treasury via SPS is protected using public key infrastructure (PKI) encryption. The information includes the payee's name, address, TIN (when applicable), and bank account information, and is shared at the time the disbursements are submitted to Treasury for execution. 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 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). This information includes the obligor's name, address, TIN (when applicable), and amounts paid and withheld. This information is shared with the IRS to support the federal income tax processing 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.

DHS is also required to share information about to debts with Treasury pursuant to the Debt Collection Improvement Act of 1996<sup>24</sup>. 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 or does include name, obligor name (for immigration bond-related debts), address, TIN (when applicable), SSN (in the case of a DHS employee), and debt amount (e.g., unpaid amount, overpayment amount). Each DHS FM System prepares batch data files that are sent electronically to 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.

The information that DHS provides to the IRS for interest payments 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.

### Department of Defense

The Coast Guard CAS Suite shares information with the Department of Defense financial management systems including: Naval and Electronics Supply Support System (NESSS), Defense Automated Message Exchange System (DAMES), Electronic Transportation Acquisition (ETA), and the U.S. Air Force Mobility Command.

### Department of the Interior

DHS has signed an interagency agreement with the DOI-IBC to be the federal shared service provider for the replacement CAS Suite for DNDO, TSA, and USCG. The DHS FSM program team is actively working with DOI-IBC personnel to prepare the FSSP for the migration of data from the Core Accounting System. Additionally, an Interconnection Security Agreement has also been signed between DHS and DOI-IBC.

### General Services Administration

DHS FM Systems have external connections with various GSA billing and payment systems to remit payments for telephone, overtime utilities, enhanced custodial services, and mechanical operations and maintenance services online payments and collections.

---

<sup>24</sup> 31 U.S.C. § 3701, and Pub L. 104-134 (Apr. 26,1996).



## External Financial Institutions

DHS FM Systems also share bank account and routing information with external financial institution “lockboxes” for processing payments and reimbursements. A lockbox is a collection and processing service provided by a financial agent that accelerates the flow of funds to DHS FM Systems and processes associated data. This service may include collecting DHS mail from a specified post office box; opening envelopes, extracting, sorting, and batching the envelope contents; scanning and capturing required data from payment instruments and remittance documents; balancing and totaling batches; recording the payments; processing the items; making the deposit; and transferring the funds. DHS FM Systems receive remittance data either in hard copy or via electronic format.

## Private Collection Agencies (PCA)

DHS may use PCAs to help collect debts owed to the Department. For example, CBP currently has over three billion dollars outstanding for various reasons, particularly debts owed to CBP in relation to importing and exporting goods.<sup>25</sup> DHS Components attempt to service the debts internally prior to referring a debt to a PCA.

### **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 functions in DHS FM Systems. All external sharing falls within the scope of published routine uses defined in the SORNs identified in Question 1.2.

### **6.3 Does the project place limitations on re-dissemination?**

There are generally no limitations placed on re-dissemination of this information. Any further sharing of DHS FM Systems data is permitted as authorized by the recipient agency’s SORN(s) or information sharing policies.

---

<sup>25</sup> This initiative is driven by intense public interest in the amount of CBP’s growing, uncollected, delinquent debt. A large majority of the debt (95% or more by dollar value owed) is corporate or commercial debt owed by a business entity of some sort (*e.g.*, corporation, partnership, LLC), rather than by an individual. CBP provides detailed debtor information to contracted debt collection services including company name, address, employer identification number, specific import information related to the debt including amount owed, as well as the names, phone numbers, and email addresses of individuals employed by or representing the debtor. In rare instances, the debtor may be an individual (person) using an SSN as his/her importer of record number, home address as business address, etc.



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

DHS uses the payment schedule dates from when batch payment files are transmitted to Treasury to track disclosures of DHS FM Systems data (including PII) outside of DHS. Upon successful transmission to Treasury, the same batch data file transmitted to Treasury is also transmitted to DHS FM Systems in order to record the payments. By recording the payment schedule date from the batch file, each DHS FM System records the disclosure of the associated records.

## **6.5 Privacy Impact Analysis: Related to Information Sharing**

**Privacy Risk:** There is a privacy risk that information from DHS FM Systems may be improperly disclosed outside of DHS.

**Mitigation:** These risks are mitigated by the fact that information maintained in DHS FM Systems is shared in a manner consistent with the routine uses prescribed in the SORNs identified in Question 1.2 or as required by law.

## **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 DHS FM Systems 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.

### **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 DHS FM Systems 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.



### **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 DHS FM Systems or be able to correct their information because they do not know which system maintains information about them.

**Mitigation:** Individuals can request access to information about them by submitting a Freedom of Information Act (FOIA) request. They may also request that their information be corrected once they have reviewed their information and discovered any inaccuracies.

**Privacy Risk:** There is a risk that because there are so many FM Systems and smaller FM Systems (see Appendix), an individual may not be able to correct, access, or amend his/her applicable records in all systems even if he/she files a request via the FOIA process.

**Mitigation:** DHS believes the PIA will enable individuals to better understand which systems house their data. As a result, individuals should be able to contact the correct Component or FOIA office for further assistance. This PIA also serves as a roadmap for FOIA professionals to locate data pursuant to a request.

## **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?**

DHS FM Systems 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. DHS FM Systems application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail discloses actions such as unauthorized access, modification, and destruction of data that would negate its forensic value.

DHS FM Systems 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 or encrypted email.



Additionally, the SSNs maintained in the DHS FM Systems for DHS employees and contractors/vendors are visible only to those authorized users with a need to know based on their user access and prescribed official duties (*e.g.*, system administrators).

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

All DHS 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 specific roles with a defined set of privileges to ensure overall system integrity. The DHS FM Systems system administrators 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 a DHS FM System, users must complete the system-specific 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 similar across all DHS FM Systems instances, including:

- *Originator* – Create and process commitments and obligations in the DHS FM Systems Desktop Screens.
- *Funding Certifier* – Review, edit, and certify commitments and obligations and check funding availability in the DHS FM Systems Desktop Screens.
- *Approving Official* – Review and approve or deny commitments and obligations in the DHS FM Systems Desktop Screens; cannot edit.
- *Payment Technician* – Create and process bills/invoices; create new vendor entries in the DHS FM Systems vendor table; and 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 DHS FM Systems instances, as necessary.



## **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). When 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 (ISA) for internal and external systems that interface with DHS FM Systems to ensure adequate protections are in place to safeguard information transmitted between systems.

### **Responsible Officials**

Chip Fulghum  
Chief Financial Officer  
Department of Homeland Security

### **Approval Signature**

Original signed copy on file with DHS Privacy Office.

---

Karen L. Neuman  
Chief Privacy Officer  
Department of Homeland Security



### APPENDIX A

In addition to the six Core Financial Management Systems described in the body of this PIA, the following IT systems are also used by DHS for the collection, use, dissemination, and maintenance of financial information from DHS employees, contractors, vendors, grantees, and members of the public.

#### DHS-wide

**DHS Treasury Information Executive Repository (DHSTIER)** (July 23, 2015): The Department of Homeland Security Treasury Information Executive Repository (DHSTIER) application collects financial data from the Components for the Office of the Chief Financial Officer (OCFO). DHSTIER receives monthly uploads of financial accounting and budgetary data from each Component's financial system and produces the Department's monthly, quarterly, and yearly reports for the Consolidated Financial Statement Audit. DHSTIER generates the Financial Statements and related Footnotes required for producing the Annual Financial Report (AFR). DHSTIER is an agency data archive that captures, validates, and maintains this data for reporting use. Editing functionality of submitted data is not permitted and it is audited annually. Each Component may only see its own data.

**Sunflower Asset Management (SAM)** (July 23, 2015): As noted above, SAM is a property management system providing primary business functions such as acquisitions, transfers, retirements, modifications, and asset tracking. SAM is integrated with Oracle Financials Fixed Assets (FA) for capitalized asset transactions.

The USCG CAS Suite relies on its own instance of SAM, but several other DHS Components use an enterprise-wide instance of SAM, owned and operated by the DHS Chief Readiness Officer (CRSO) and available to DHS Components. Sunflower is fully integrated with the Oracle Financials FA module for capitalized asset transactions; however, it is not considered to be a module of Oracle Financials because it was developed by a third party. SAM functions include:

- Property management system, which provides the primary business functions like Acquisitions, Transfers, Retirements, Modifications, and Asset tracking;
- Integrated with Oracle Financials Fixed Assets for capitalized asset transactions;
- FPD is integrated with Sunflower by providing the purchase order and/or receipts to create assets;
- PPC Checkfree Subsystem; and
- Supports the reconciliation of military payroll with four reconciliation sets and a single general ledger.



### U.S. Customs and Border Protection (CBP)

**Electronic Collections System (ECS)** (June 10, 2019): ECS is a point-of-sale system consisting primarily of cash registers and workstations located at all U.S. ports of entry (POE) and several overseas pre-clearance locations. CBP uses ECS to collect revenue in the form of duties, taxes and other fees associated with products entering the United States. Individuals may pay for such fees with cash, a check, or a credit card. ECS sends credit card transaction authorization requests to a national credit card processor (processing bank). These requests include an encrypted package of the customer's name, credit card number, transaction amount, and transaction number. A new six-digit authentication code and an eight-digit bank code is generated for each transaction each time a credit card is swiped. The processing bank returns an encrypted message back to the authorization-requesting cash register with an approved or denied message for that transaction.

CBP may collect the following information in ECS in association with a payment:

- CBP Importer Record Number or Tax ID Number (or Social Security number (SSN))
- Credit card holder name
- Last 4 digits of the credit card number
- Credit Card transaction number
- Amount of transaction
- Time and date of the transaction
- CBP Port number
- Driver's license number, travel document number, or other identification as required to associate a payment with an individual.

The collection and storage of SSNs occurs on a limited basis when the payee pays by check and provides SSN as an identification number if he or she does not have a tax ID or unique CBP Record Number. The SSN is stored in ECS to comply with Department of Treasury directives and is ultimately used for the purpose of debt collection. No credit card numbers are retained by ECS. Only truncated credit card numbers are used to identify the card number associated with a transaction in accordance with Payment Card Industry (PCI) compliance.

ECS will be transitioned to a new system using a phased approach over several years. The new system, POS, will be discussed further below.

**National Data Center (NDC) Administrative Applications** (July 23, 2015): The NDC Administrative Applications (NDC Admin Apps) are a collection of administrative applications that operate under the umbrella of the CBP Mainframe architecture in order to perform their mission-specific functions. They carry out an array of administrative functions related to system security, as well as providing specific support to personnel processes. The Personnel Action Request Tracking System (PARTS) Human Resources Management (HRM) personnel system



enables Human Resources (HR) staff and field users to initiate, electronically transmit, track, and monitor CBP personnel actions to completion.

The NDC Admin Apps collect the following PII about CBP employees: SSN; Name; Employee's Birthdate; Employment Status; Military Information; Current Address; Salary Information; and Bank Account number.

**National Finance Center (NFC) System (NFC-LAN)** (July 23, 2015): The CBP National Finance Center (NFC) LAN system is a general support system consisting of desktop computers, laptop computers, printers, multi-function devices (copy/print/scan/fax), portable media (CDs, DVDs, flash drives, external hard drives), and peripheral devices (scanners, digital cameras, webcams, etc.) all connected to the CBP local area networks deployed throughout the NFC campus. The NFC campus serves over 700 personnel at the Financial Management Services Center located in Indianapolis, Indiana. The NFC LAN System provides basic platform access to all the CBP and DHS information systems and major applications, while simultaneously enabling ad-hoc applications and usage scenarios that support the mission requirements.

CBP employees and contractors use the NFC LAN System to access file storage via Windows File and Print (WFP System), the email system via Email as a Service (EaaS), and perform financial resources management via applications such as the Automated Commercial Environment (ACE), Systems, Applications, and Products in Data Processing (SAP), and the Automated Commercial System (ACS). These applications are not included in the NFC IT boundary, and each application is responsible for its own compliance documentation.

The NFC requires employees and contractors to collect, process, transmit, and store structured and unstructured ad-hoc information such as reports, lists, presentations, and memos that cannot be categorized or assigned to any other defined program. Every office and every role of the NFC may be required to execute tasks and functions that require the production and processing of this type of data. Although PII may be stored on this hardware, such as local hard drives and portable media, the PII is almost exclusively personal records or case notes, rather than records in a system of records.

The NFC LAN does not directly collect or store any personally identifiable information. The system does contain sensitive financial information.

**NDC Financial Applications (NDC Financial Apps)** (July 23, 2015): The NDC Financial Applications are a collection of three (3) administrative CFO-designated financial applications. These applications operate under the umbrella of the CBP Mainframe environment in order to perform their mission-specific functions. The individual system descriptions are as follows:

1. COSS: The CBP Overtime Scheduling System (COSS) is the official Time and Attendance system used by CBP for Payroll. This legacy application is a key component required to effectively manage workforces' schedule and overtime workload. COSS is part of a



collection of administrative applications that execute on the CBP Mainframe architecture to perform mission functions.

2. TAMS: The Time and Attendance Management System (TAMS) is the timecard system that was the predecessor to COSS and supports COSS for payroll processing. TAMS is used to interface with USDA for schedule transmissions. It is no longer used for timecard entry.

A third application, the Automated Scheduling Tool (AST) (formerly known as Telestaff) is no longer part of the NDC Financial Apps boundary but contributes to the same functions. AST is a web-based scheduling tool used to manage the work and overtime schedules of CBP law enforcement officers in the Office of Field Operations (OFO) in concert with staffing needs and union bargaining rules. The capability provides built-in alerts and enhanced transparency to aid in compliance with CBP union bargaining rules, as well as auditing capabilities to track schedules and overtime.

In total, COSS and TAMS provide the following functions: a payroll interface, time and attendance, work tickets, and scheduling capability. COSS currently interfaces with TAMS in order to transmit the time and attendance data to USDA for payment. SSNs are used as the unique personal identifier for employees in COSS and TAMS because USDA still requires SSNs to capture and identify payroll and earnings data for a given employee. The PII received from the USDA Bi-Weekly download file includes the following employment information about CBP employees: SSN; first and last name; agency; organization code; duty; city; job series; cost center; hire date; supervisor code; date of birth; grade; step; and salary. COSS and TAMS also retrieve information using the following personal identifiers for CBP employees: birthdate; employment status; full name; military information; current address; salary information; SSN; and hash IDs. Because AST is used to manage work and overtime schedules, and not for payroll purposes, it does not collect SSNs.

### **Revenue Modernization Program**

The Revenue Modernization Program is a new effort to improve the revenue collection processes at CBP ports of entry (ports of entry (POEs)). By implementing automated and electronic payment methods, improving systems integration, and implementing new technologies, Revenue Modernization will allow CBP Officers (CBPOs) and field personnel to spend less time performing rote revenue collection and allow more time performing mission-critical customs enforcement activities.

**Electronic Payment Options (ePO)** (January 31, 2020): ePO is an effort to leverage existing payment options, such as Pay.gov, to enable trade and travel related payments to be made online via the eCBP website (e.cbp.dhs.gov). Current functionality focuses on maritime fees and allows prospective brokers to register for and take the Broker Exam subsequent to paying the associated fees. Future planned features include automated data entry into Automated Commercial



Environment (ACE); pre-validation of data to eliminate errors; and the ability for customers to make payments through multiple payment options, including Pay.gov, PayPal, credit and debit cards, Amazon Pay, and in the future, Automated Clearinghouse (ACH).

The system architecture is designed to collect any type of online fee for CBP. The eCBP website allows users to complete various forms online and submit the respective fee payments via the Pay.gov site. The site currently accepts broker exam registrations, and future additions will include license applications, permit and annual permit renewals, triennials and trade and traveler fees. The payment data entered on eCBP website will be saved in the Mobile Collections and Receipts (MCR) repository (discussed below), which is the backend database for e.cbp.dhs.gov. Most, if not all, forms that will be filled out by the public on eCBP contain PII as they deal with brokers, importers, and passengers.

ePO collects the following data fields in support of the broker license exam registration and payments:

- Exam Fee Receipt Number;
- Fee Amount;
- Date Paid;
- Application/Submission Date;
- Exam Date;
- Withdrawal Date;
- Notification Date;
- Exam Score;
- Appeal Date;
- Exam Remarks (Free form field to indicate a reason to edit information and submit cancellation or withdrawal);
- Exam Status (Drop Down Menu: Pass/Fail);
- Is the Applicant a U.S. Citizen? (Yes/No);
- Has the Applicant Attained 18 years of age? (Yes/No);
- Is the Applicant an Officer or Employee of the United States? (Yes/No);
- Name;
- Date of Birth;
- Social Security number;
- Birthplace City, State, and Country;
- Residence Street Address, City, State, Zip Code, and Country;
- Mailing Street Address, City, State, Zip Code, and Country;
- Contact Information: Primary and Business Phone Numbers; and
- Email Address.



**Mobile Collections and Receipts (MCR)** (January 31, 2020): MCR is an internal-facing mobile application that allows payments to be accepted in an environment that does not have a cash register. This system replaces paper forms and receipts with an electronic receipt and serves as the backend repository to the public-facing eCBP web portal. MCR gives CBPOs automated capabilities to collect several types of fees including maritime, immigration, duties, and taxes, and allows CBPOs to send receipts for CBP Forms 368 and 1002 to customers via email. MCR receives payer-specific data from the ACE/Automated Commercial Services (ACS)/Vessel Management System and sends collections data to the Systems, Applications, and Products (SAP) financial system.

**Point of Sale (POS)** (January 31, 2020): POS is an upgrade of the legacy ECS that will be deployed in a phased approach to the POEs over the next two years to close major financial security gaps, improve payment processing, add new payment options, and enable each point of sale register to connect directly to the CBP network. POS was introduced to replace ECS and will run concurrently for a period of time until POS is fully operational.

The following data fields are collected from members of the traveling public:

- CBP Importer Record Number or Tax ID Number (or SSN);
- Driver's License Number;
- Credit card holder name;
- Last 4 digits of the credit card;
- Credit Card transaction number from Vantiv/WorldPay LLC;
- Class Code(s) collected and Amounts of each collection transaction;
- Time and date of each transaction;
- CBP Port number; and
- Reference Data associated with the transaction.

**Smart Safes** (January 31, 2020): Smart Safes are safes that automatically accept, validate, record, and store cash in a secure environment. Smart Safes are intended to reduce the labor-intensive manual processes surrounding cash handling at POEs, and will modernize collections in the field by allowing cash deposits to be counted and counterfeit cash to be identified. Smart Safes are able to electronically deposit funds in the bank for Treasury. A CBPO must login via an individual user ID and password before each transaction can take place, which ensures that all transactions are reconciled and auditable. When deposits are made, the safe records and tracks each deposit while automatically checking for counterfeit cash. Once in the safe, the cash becomes the property of the bank and the cash is collected by courier on a prearranged schedule or when the safe reaches a predetermined limit.

**Federal Emergency Management Agency (FEMA)**



**Automated Acquisition Management System (AAMS)** (July 23, 2015): The Automated Acquisition Management System (AAMS) is a COTS product used by personnel in FEMA's Office of the Chief Procurement Office as the agency's contract management system.

AAMS is a web-based application that manages and stores acquisition data and captures acquisition information including notes, data, attachments, commitment documents, and milestones. The information is then organized into tabs for storage and reference. AAMS also formats data and creates acquisitions related documents. AAMS receives commitment documents from FEMA Program Office users via the Integrated Financial Management Information System (IFMIS) in the form of purchase requests, which are used to generate award documents that are then passed back to IFMIS as obligations. These award documents are federal contracts issued between FEMA and vendors or other agencies in accordance with the Federal Acquisition Regulation (FAR).

**Payment and Reporting System for Grantees (PARS)** (July 23, 2015): The Payment and Reporting System (PARS) is comprised of two PARS application servers and the three PARS web servers. PARS resides within the IFMIS accreditation boundary as the web-based "front end" to the IFMIS database. As part of the front end functionality, PARS collects PII and pushes it through to the Web-IFMIS database where information is maintained. PARS enables grant recipients to submit requests for grant payments as well as submit financial status reports using an online representation of OMB Standard Form 425.

### Federal Law Enforcement Training Center (FLETC)

**Infrastructure and Enterprise Management Tools (IEMT)** (July 23, 2015): The Infrastructure and Enterprise Management Tools System (IEMT) provides infrastructure and management to Information Technology (IT) network applications and services. This includes the Administrative, Wireless, Telecommunications, and DMZ networks used by authorized FLETC personnel, contractors, and partner organizations at the following FLETC facilities: Glynco, GA; Artesia, NM; Charleston, SC; Cheltenham, MD; Manhattan, KS; and Washington, D.C. The Administrative LANs at each site are connected via the DHS OneNet WAN to provide customers with an enterprise platform to receive IT services. The wireless LANs provide customers with IT capabilities. The Telecommunications LAN provides customers with phone, fax, and voicemail services. The voice network traverses a private Avaya managed network as well as a logically separated portion of the FLETC infrastructure to provide IP-based communications. The DMZ offers capabilities to all FLETC sites to share enterprise management services, training capabilities, and application services.

The management tools collect logging information for all devices. These logs include usernames and passwords. Several IEMT subsystems collect the following employee PII during the normal course of operations:



- Active Directory collects name, title, address, phone number, Component, email address, username and password, account profile, permissions, and user groups.
- The modular messaging system collects phone messages.
- The management tools collect logs for all devices. These logs include usernames and passwords.
- Exchange collects emails for all account holders.

### Immigration and Customs Enforcement (ICE)

**Electronic System for Personnel (ESP)** (July 23, 2015): ESP is a web-based system installed on a centralized application web server. ESP automates the processes involved in managing ICE personnel actions (Using Standard Form SF-52). SF-52s are used to establish and maintain data pertaining to employment and payroll administrative functions. The system provides the capability for the ICE Human Capital Office (OHC) to electronically create, edit, submit, copy, delete, and maintain a history of personnel actions; establish workflow of personnel actions depending on type and originating office within ICE; create an electronic routing sheet; return personnel actions to the originator; and make comments concerning personnel actions. ESP also tracks the status of personnel actions. Personnel action data are supplemented by OHC with position classification information data. Once the SF-52 is finalized within ICE, the data is submitted to the USDA NFC for processing to effectuate changes to the personnel and payroll data for the ICE employee for whom the SF-52 was issued. When finalized, an electronic SF-52 mirrors the Notice for Personnel Action (SF-50).

**FileOnQ** (July 23, 2015): FileOnQ provides a database and repository for invoices, bonds, reimbursable agreements, obligations, field deposits, and related documents. Using FileOnQ, data can be queried and tracked via invoice number or vendor ID, reports can be generated by support personnel, and financial actions can be executed by users. FileOnQ obtains information through three different types of manual uploads:

1. The ICE eBONDS system provides surety bond information. The bond information is downloaded to a shared drive and then uploaded into FileOnQ via a manually initiated import utility.
2. Payments and invoices from other federal agencies such as the Treasury are sent to the Burlington Finance Center via the standard Intra-government Payment and Collection (IPACS) import utility or electronic transfer. Then, the information is entered into a spreadsheet by the accounting technician on a daily basis and uploaded into FileOnQ.
3. For invoices and documents sent via email, mail, or FAX, the accounting technician creates a file in FileOnQ, scans the documents (if not already a PDF file), and uploads the document into the created file.



Approximately, ninety-five percent (95%) of the data entered into FileOnQ is obtained through this last method, e.g., cash bonds, invoices, agreements, obligations, field deposits.

Once the invoice is ready for submission for payment, the invoice number is copied from FileOnQ and pasted into the ICE Federal Financial Management System (FFMS). The accounting technician then manually enters the remaining information into FFMS for processing.

FileOnQ collects general contact information such as addresses and telephone numbers from businesses. Occasionally, personal information is submitted on invoices in lieu of business information. The system may also contain SSNs when included on submitted invoices. For bonds, the documents can also include personal addresses and telephone numbers along with alien numbers.

**OFM Online** (September 21, 2016): OFM Online is an internal SharePoint site used by U.S. Immigration and Customs Enforcement (ICE) Office of Financial Management (OFM). The site provides financial policy and related information to the financial community within ICE and other DHS components for which ICE provides financial services. Individuals use OFM Online to research financial policy, process, and procedural information, access links to other applications and sites, download forms to submit via fax or email, and complete and submit certain web forms via OFM Online to the ICE Dallas Finance Center.

The following four forms that users submit to the ICE Dallas Finance Center via OFM Online contain PII, as specified below:

- Employee Payment Information Form: DHS Point of Contact information (name, email address, phone number); employee name, TIN/SSN; employee phone number, employee job title; employee mailing address; bank account number; bank routing number.
- Vendor Payment Information Form: DHS Point of Contact information (name, email address, phone number); Dun and Bradstreet Universal Numbering System (DUNS) number; TIN/SSN; vendor number; bank account number; bank routing number.
- Extension of Time to Sell/Purchase Real Estate Form: Employee name; duty station location; mailing address; telephone number; email address.
- Temporary Quarters Subsistence Expense (TQSE) Actual Expense Worksheet: Employee name; spouse name; names and ages of dependents.

These forms are only available on the ICE intranet, and can only be completed by ICE employees and contractors who have access to the site.

**Real Property Management System (RPMS)** (July 23, 2015): The Real Property Management System (RPMS) replaced a disorganized set of ad hoc tools used by ICE Office of Asset Management (OAM) and Office of Co-Location (OCL) to coordinate the acquisition, management, disposition, and accounting of ICE real property assets. RPMS provides enhanced



project management and tracking tools to the ICE office responsible for managing ICE leased and owned properties, overseeing active projects including new space requests, construction, build-to-suit projects, leases, various infrastructure space actions, and executing ICE repair and alteration projects.

RPMS collects and maintains limited ICE employee, contractor, and public data for planning and tracking purposes, such as: name, job title, grade, program office/department, organization/company, email address, office phone number, employment type, and IRMNet UserID (if applicable). RPMS generates reports from this data for statistical purposes to support facilities and asset management functions.

**I-901 Fee Collection Services System** (June 30, 2017): The web-based I-901 Fee Collection Services System (I-901 System), as of September 2012, is managed by the U.S. Immigration and Customs Enforcement (ICE), Student and Exchange Visitor Program (SEVP). Previously, the U.S. Department of the Treasury, Financial Management Service (FMS) managed the I-901 System. FMS is still responsible for collecting the fees and for their proper disposition. The I-901 Fee was established by Congress, which mandated the implementation of a fee to be paid by prospective nonimmigrant students and exchange visitors and their dependents seeking F, M or J status (I-901 Fee), to defray the operation and maintenance costs incurred by SEVP. The I-901 System is covered by the DHS/ICE-001, Student and Exchange Visitor Information System (SEVIS) System of Records Notice.<sup>26</sup>

The I-901 System serves four purposes: (1) allows applicants to pay the required I-901 Fee; (2) allows applicants to check the status of a previously submitted I-901 payment; (3) allows applicants to print proof of payment (I-901 Payment Confirmation) to present at a visa appointment; and, (4) is a source for detailed information/instructions regarding the I-901 Fee.

The I-901 System is comprised of the following components to support payment of the I-901 Fee:

1. A web-based payment system whereby a contracted financial institution hosts an Internet-based electronic version of the I-901 Fee Transmittal Form that allows an individual to file the Form I-901 and pay the I-901 Fee through a credit card interface to FMS's Pay.Gov credit card portal.
2. A lockbox payment mechanism whereby a person can mail a completed Form I-901 and associated payment to a lock box hosted by the contracted financial institution.
3. A bulk filing capability whereby authorized Exchange Visitor Programs can upload a file of exchange visitor data and charge the payment via Automated Clearing House (ACH) debit to a predetermined sponsor bank account.

---

<sup>26</sup> DHS/ICE 001 Student and Exchange Visitor Information System 75 FR 412 (Jan. 5, 2010).



4. A Western Union payment mechanism whereby a person can remit the I-901 data and associated payments at a local Western Union office.

The I-901 System involves interactions between DHS ICE SEVP, FMS, and the contracted financial institution in order to complete I-901 Fee transactions.

In addition to administering the I-901 System, SEVP is also the owner of Student and Exchange Visitor Information System (SEVIS), an Internet-based system that maintains real-time information on nonimmigrant students and exchange visitors, their dependents, and schools and sponsors that host these nonimmigrants. Payments received from F, M and J nonimmigrant applicants are validated against SEVIS records to ensure that the payment is posted to the appropriate SEVIS record, and that the applicant is given proper credit for having paid the required I-901 Fee. Additionally, the validation with SEVIS is used to accurately identify individuals for visa issuance and entry into the United States. FMS is responsible for the collection of I-901 Fees and their proper disposition.

The contracted financial institution, an SEVP contractor, serves as an agent for the government to administer, host, manage, and operate the I-901 Fee site. The contracted financial institution also provides support services to the I-901 System by processing Form I-901 applications and I-901 Fee payment transactions; supports reporting capabilities, applicant inquiry and status information, applicant information updates and financial reconciliation.

### Transportation Security Administration (TSA)

**Electronic Time and Attendance KRONOS (ETA KRONOS)** (July 23, 2015): ETA Kronos is an automated and standardized labor management solution that operates within the TSA Operating Platform (TOP) environment. The system is deployed at all airports for purposes of recording employee clock in/out times and transferring that information to appropriate payroll and human resource systems. Individuals access the system by swiping a TSA issued KRONOS ID card. The system also requires the user register his or her physical presence by placing a finger on a scanner tab that converts the individual's fingerprint to a fingerprint template that is not logged or stored in the system. The template measures fingerprint minutia/data points and converts the information using a mathematical representation that provides a one-to-one match to the employee. The technology prevents the recreation of a full fingerprint from the template.

In order to provide anti-spoofing measures, the system also records several electronic inputs from the user's skin to obtain for example: temperature, humidity, impedance, and other bio-measurements. The technology immediately rejects fake fingers. The Kronos 4500 Touch ID terminal uses a sub-surface technology that images below the surface layer of the skin.

The system collects the following PII from TSA employees: name, date of birth, fingerprint template and non-PII anti-spoofing data points, user ID, and location and clock-in/out times for purposes of recording hours worked. The system contains encrypted SSNs for the purpose of



interoperating with other payroll systems that require this information. The system also contains non-sensitive PII data such as shift supervisors and general scheduling information.

## U.S. Coast Guard (USCG)

**Asset Logistics Management Information System (ALMIS)** (July 23, 2015): The Asset Logistic Management Information System (ALMIS) enables efficient, flexible, and cost-effective aircraft and surface force operations, logistics, and maintenance support. ALMIS supports data entry from the start of a mission, recording the mission execution, tracking crew events, asset aging, asset configuration, asset maintenance requirements, asset part replacements, warehouse activities, and procurement actions.

ALMIS supports the comprehensive maintenance, operations, and logistical support of Coast Guard aircraft at 28 Coast Guard air stations, and the Aviation Logistic Center (ALC). In addition to Coast Guard aviation, ALMIS is currently supporting small boat forces and patrol boat forces with anticipation of cutter fleet, electronics, and shore assets over the next several years. ALMIS has over 19,000 registered users that include air crews, surface force crews, maintainers, contractors, and senior decision makers at Coast Guard Headquarters.

**Fleet Logistics System (FLS)** (July 23, 2015): The Fleet Logistics System (FLS) is designed to automate the management of USCG cutter and small boat logistics, which includes Configuration Management (CM) maintenance actions, procurement and supply activities, automated Requisition Management (RM), Coast Guard Parts Availability Research Tool (CG-PART), and associated financial transactions. CG-PART is a web based inventory locator tool that allows individuals to search by National Item Identification Number (NIIN), Federal Supply Code (FSC), Commercial And Government Entity (CAGE) code, part number, or Cognizance Code (COG). Search results provide the location and quantity of the item. FLS is also integrated with other enterprise systems, to include the Naval and Electronic Supply Support System (NESSS), the Naval Engineering Technical Information Management System (NE-TIMS), the FLS Mobile Asset Manager (MAM) application, and Financial and Procurement Desktop (FPD).

FLS collects name, rank, employee ID, phone numbers, email addresses, and work addresses from USCG employees and contractors.

**Integrated Aids To Navigation Information System (IATONIS)** (July 23, 2015): Integrated Aids to Navigation Information System (IATONIS) is the USCG system used to store pertinent information relating to short range aids to navigation. There are five components of IATONIS used to collect personal information: Private Aid to Navigation Owner Contact Information, Wreck Owner Contact Information, Oil Rig Owner Contact Information, Private Property Owner Contact Information, and USCG Auxiliary Member Contact Information. This information allows the Coast Guard to contact owners of wrecks, oil rigs, private aids to



navigation, private property owners on which an aid to navigation is located, and operators of oil rigs. If the owner designates another individual as the point of contact for the Coast Guard, the point of contact information is retained as well.

IATONIS is a privacy sensitive system which collects limited contact information from members of the public in order to distribute information and perform various other administrative tasks. Information collected may include name, office address, office email, and office phone for persons or organizations that can be contacted for information related to private wrecks, oil wells, private aids, and leased private land.

**Joint Uniform Military Pay System (JUMPS)** (July 23, 2015): The Joint Uniform Military Pay System (JUMPS) is a custom designed military payroll system used for computations of all necessary information used to pay active duty, reservists, and retired military members. This is an IBM Z/OS Mainframe based system, with encrypted terminal connections for the clients. JUMPS collects PII from USCG employees and contractors only, including SSN.

**Naval and Electronics Supply Support System (NESSS)** (July 23, 2015): The Naval and Electronics Supply Support System (NESSS) automates the maintenance and logistics management of USCG assets including cutters, small boats, and shore based facilities. NESSS is described as an Information Resource Management (IRM) system. NESSS is an Oracle-based database system used primarily by the USCG Yard and the Surface Forces Logistics Center. NESSS is an integral part of the Vessel Logistics Systems (VLS), which include the Automated Requisition Management System (ARMS), Coast Guard Parts Availability Research Tool (CG-PART), Configuration Management plus (CMplus), and the Fleet Logistics System (FLS). NESSS incorporates approximately 12 external interfaces with USCG and United States Navy (USN) systems and over 1,000 application modules. NESSS was originally designed to move a myriad of legacy applications off aging hardware and has now evolved into a fully integrated system linking the functions of provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance and property accountability, and a full financial ledger. The system is completely matrix driven, allowing maximum user configuration and adaptation. The system contains the following modules for use by its end users: Supply, Finance, Procurement, Depot, and Provisioning/Unit Configuration. The various NESSS accounts provide its approved end users with the capability of inserting, deleting, editing, or viewing any relevant data concerning USCG Supplies.

NESSS collects the following personal information from USCG employees: names, business addresses, business phone numbers, business email addresses, and employee pay rates.

**Shore Asset Management (SAM)** (July 23, 2015): The Shore Asset Management System (SAM) utilizes a suite of COTS Enterprise Asset Management (EAM) software products comprised of IBM MAXIMO and TRIRIGA to provide maintenance, project, and inventory functionality to USCG Civil Engineering (CE), Facilities Engineering (FE), and Real Property



(RP) communities. SAM is available to shore-based USCG units and provides detailed planning information such as work plans, schedules, costs, labor, materials, equipment, failure analysis, and related documents by utilizing a work order tracking component. The software allows the scheduling of work orders based on real-time updates of criticality.

SAM provides real-time display of work orders and individual assignments using a work manager dispatch component. This allows supervisors and planners to interactively manage upcoming work by taking into account factors such as job priority and workforce availability. SAM tracks equipment, associated costs, histories, and failures of any serialized piece of equipment as it moves through a facility. A Preventive Maintenance (PM) component generates work orders individually, in batch, or automatically.

SAM provides core information about USCG shore facility assets. It tracks activities and assists in management of the CE Program. The information helps the CE Program manage the full life-cycle of the shore facility assets and adjust to CG mission needs. The following employee data may be collected in SAM: name, work address/telephone/email, position title/department/supervisor, date of birth, hire date, termination date, next/last evaluation dates, and pay rate.

**Windows Integrated Automated Travel System/Travel Preparation and Examination (WINIATS/T-PAX)** (July 23, 2015): The Windows Integrated Automated Travel System/Travel Preparation and Examination (WINIATS/WEBTPAX) is a USCG-configured COTS application. The users in the field have the ability to access WEBTPAX via the USCG intranet (via a web browser) for creating orders and submitting their travel claims for Temporary Duty Travel. Users must have an Authorizing Official review and approve their claim in WEBTPAX before it can be released. When the claim is approved, it along with any associated data is moved to WINIATS for calculation and payment. WINIATS ensures that payment data is correct and determines the amount the traveler is due to be paid. When this calculation is complete the payment amount is transmitted to the Finance Center in Chesapeake Virginia for payment to the member via EFT. The Pay and Personnel Center also receives Temporary Duty travel and Permanent Change of Station travel claims via hardcopy. These claims are entered into WINIATS for calculation and payment. The payment is transmitted in the same manner as the claims described above. The WINIATS/WEBTPAX user base is all active duty, reserve, and civilian employees of the Coast Guard (approximately 37,000 active duty, 8,000 reserve, and all civilians).

### **United States Citizenship and Immigration Services (USCIS)**

**E-Filing (Electronic Filing System)** (July 23, 2015): E-Filing is a web-based tool that supports USCIS mission efficacy and efforts towards greater public transparency by providing a mechanism for individuals or authorized parties acting on behalf of individuals (referred to herein collectively as “applicants”) to submit applications and petitions (referred to herein collectively as “applications”) for certain immigration benefits and services directly to USCIS. E-Filing



eliminates the need for some applications to be submitted to USCIS in hard-copy and then manually input by USCIS staff into the CLAIMS system. Data submitted to USCIS through e-Filing is used to assist USCIS examiners in corroborating information provided by applicants, thereby ensuring that the process is consistent with all applicable laws and regulations. This data is used to perform background checks, examinations (review of the information that is being provided by applicants), and adjudications (process by which decisions are made to grant or deny an application).

The e-Filing System collects the following personally identifiable information from applicants: name, country of citizenship, date of birth, present address, receipt number, SSN, A-Numbers, country and place of birth, work authorization information, credit card name and expiration dates, port of entry, form type for benefit applied for, sex, phone number, family members, photo, signature, passport information, interview codes, and history codes.