Privacy Impact Assessment
For the

Core Accounting Suite

September 18, 2009

Contact Point
Chuck Lewis
United States Coast Guard
Finance Center
(757) 523-6905

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

Abstract

The United States Coast Guard (USCG) Finance Center (FINCEN) maintains the Core Accounting Suite, an integrated financial and asset management system designed for use by three Department of Homeland Security (DHS) agencies: the USCG, Transportation Security Administration (TSA) and Domestic Nuclear Detection Office (DNDO). The purpose of this PIA is to document how the USCG FINCEN collects and maintains personally identifiable information (PII) within the Core Accounting Suite.

Overview

Core Accounting Suite is a financial suite of applications hosted at the USCG FINCEN. The Core Accounting Suite's primary objective is to support FINCEN's mission of providing financial and data warehousing services to the USCG, TSA, and DNDO.

Connection to PII

Several elements of the Core Accounting Suite involve PII. These elements are necessary to process the myriad of financial transactions within the Core Accounting Suite. The elements may consist of user names & addresses, user bank account numbers & routing numbers and vendor information, such as business name, account number and banking information.

The Core Accounting Suite is a financial transaction system. These financial transactions directly affect the mission of the USCG FINCEN. The Core Accounting Suite tracks: the financial cost of what is purchased, delivered, and paid; how much cash is received; and the financial cost of assets and projects. All financial transactions are consolidated in the Core Accounting Suite so that they can be reported to DHS.

Information in the Core Accounting Suite data stores must be protected from unauthorized, unanticipated, and unintentional modification. Such modification can result in financial hardship to DHS, legal liability, and embarrassment. FINCEN is the central location within the USCG for receiving invoices and paying bills. The FINCEN provides those services, as well as many other financial services, to the USCG, TSA, and the DNDO.

The Core Accounting Suite is categorized as a major application consisting of six major subsystems and multiple financial supporting applications that are collectively referred to as the Core Accounting Suite. These subsystems are:

- Chief Financial Officer (CFO) Tools - Web-based tools used in the USCG financial community to assist with Budget Execution, i.e., Open Obligation Validation Application, Pipeline Certification Tool, and Budget Metric Tracking System
- Core Accounting System - Oracle Federal Financials (OFF) (a COTS product that includes Accounts Receivable, Assets, Projects, Inventory, Accounts Payable, Purchasing, and General Ledger)
- Financial Procurement Desktop - Enterprise-wide accounting and procurement system assigned to assist in funds and procurement management system which feeds the Core Accounting System

- Contract Information Management System - Contracts management feeding the Finance and Procurement Desktop system
- Workflow Image Network System (WINS) - Imaging and document processing system feeding the Core Accounting System
- Sunflower Asset Management (SAM) - Property management system used by TSA

The information below provides a detailed description of each of the subsystems.

Subsystems

CFO Tools: During the FY06 DHS/USCG Financial Audit, DHS auditors submitted findings and recommendations to USCG management related to the undelivered orders (UDO) validation and verification process. As a result of these findings, the USCG Office of Resource Management (CG-83) developed the web-based CFO Tools as part of the Financial Management Transformation Project. CFO Tools support financial planning, management reporting, and budgeting activities. CFO Tools is a web-based application used in the USCG financial community to assist with Budget Execution, i.e., Open Obligation Validation Application (OOVA), Pipeline Certification Tool (PCT), and Budget Metric Tracking System (BMTS). The applications are independent of each other however, collectively they provide leadership with the visibility of budget execution.

OOVA was developed to provide a tool utilizing data from the Core Accounting System in order to properly validate open obligations, and to serve as a historical record for audit purposes. The application pulls open obligations from the FINCEN Core Accounting System and provides an instrument that can classify the document as either 1) problematic distribution, 2) financial error, 3) no longer needed for its original purpose, or 4) still valid.

PCT is a web-based certification application that contains Finance and Procurement Desktop and Core Accounting System data. PCT incorporates accountability and accuracy while minimizing the amount of time required to certify accounts. The primary advantages provided by this application include: 1) accountability by senior management over assigned financial accounts; 2) improved stewardship; 3) major savings potential through significant reductions and loss of funds by rescission or mistakes; and 4) achieving CFO audit compliance.

BMTS facilitates the tracking of performance on indicators to guide financial management reforms and target resources to areas where better stewardship is needed. Within the tracking system, the metric characteristics consist of relevance, understandability, comparability, timeliness, consistency, and reliability. Using these characteristics as a foundation, the BMTS website assists finance managers with ensuring timely reconciliations, validation of unresolved documents, validation of undelivered orders, and meeting spend down rates.

Core Accounting System: The Core Accounting System is a multi-organizational implementation, processing accounting for three DHS Components: USCG, TSA and DNDO. The Core Accounting System processes Accounts Receivables, and Accounts Payable through electronic transfer. The Core Accounting System is an implementation of Oracle Federal Financials. 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 following DHS user community: USCG, DNDO, TSA).

The Core Accounting System is designed to provide users with the ability to browse, retrieve, consolidate, analyze and present information that resides in the Core Accounting System database using one-day-old information. The functions of the Cores Accounting System include:

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

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 that FPD does includes:

- 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 which 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 between 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.

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.

The USCG does not use CIMS for generating purchase requests or processing simplified acquisitions. USCG utilizes the following CIMS modules:

- Milestone Planning;
- Multiple Award Setup;
- Solicitations for bids on large contracts with option years;
- Awards (Contracts, Delivery/Task Orders, Purchase Orders);
- Blanket Purchase Agreements (BPA) & BPA Calls;
- Military Interdepartmental Purchase Request;
- Modifications, this module is used for tracking Contract Modifications increases or decreases to the obligation amounts; and
- Contract Closeouts.

Workflow Information Network System (WINS): WINS is the FINCEN's 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 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 is a system where vendors, active duty USCG persons and civilians submit documentation for reimbursement. The information is submitted by vendors and individuals who are requesting payment or reimbursement from USCG. As stated above, for paper documents and fax images received, relevant data elements are entered into the system and associated with the document image in WINS.

WINS is a feeder system into the Core Accounting System, processing accounting for the USCG, TSA, and DNDO. WINS provides the functionality of electronic submissions for reimbursements. WINS accepts electronic copies of reimbursement requests and also converts paper copies submitted into digital images for further processing in the Core Accounting System. PII is submitted by the individual or company requesting funds to make sure that the identity of the person requesting the funds can be verified and checked for authorization and appropriateness. Electronic copies submitted via FTP from the field to

WINS. An individual will check the submitted electronic document and assign it to the appropriate financial management workflow for processing. Paper submissions are mailed to the FINCEN from the field. A technician scans the paper copy into WINS and assigns the appropriate financial management workflow for further processing.

Sunflower Asset Management (SAM): 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.

While 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, 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. The following modules comprise SAM:

- Inventory Assets: Assets In-Service and assets used for recording and maintaining all active assets.
- Excess Assets: Assets used for the asset retirement process, screening periods, or logging process can be described with this module.
- Agreement Assets: Assets used to track leases, warranties, property passes, loan-ins, and external loans.
- Inactive Assets: Assets under repair, held for future use, and pre-accepted.
- Review Campaigns: Campaigns used for maintaining inventory and barcode scanning.

Typical Transaction

The Core Accounting Suite processes all accounting transactions via CFO Tools and Oracle Federal Financials. The transactions are generated and processed using data entry, document scanning and electronic transfer. The Core Accounting System, which is the accounting portion of the Suite, processes Accounts Receivables, and Accounts Payable through electronic transfer. Other portions of the Core Accounting System use a front end custom application interface to capture date entry transactions from the field.

FPD uses a custom front end application interface to create procurement documents and manage contracts. Once the data entry portion has been captured in FPD, an electronic interface moves the data from FPD into the accounting system.

WINS is the image creation system used to capture invoices. Vendors mail, fax or send invoices electronically into the WINS system. Once the transactions have been captured electronically via scanning or received via electronic transmission, the documents move through the WINS system via the MarkView and SQL Flow applications. These applications direct the invoices to the correct processing station by parsing each document type. Once the invoice has been properly validated, a transaction is created and is electronically transmitted into the accounting system for payment. Batch transfers are created and transferred to Treasury for payments to vendors.

The following is a list of possible transactions in the *Core Accounting Suite*.

- costs of purchases
- information about receivables and collections
- status of deliveries and payments
- property management
- government purchase card billing and payment
- budget reconciliation
- contract management
- payroll
- medical invoicing
- energy and other utility reports
- financial costs of assets and projects

A number of different types of operations can take place in the Core Accounting Suite. Below are two examples; note that these examples do not include all possible types of operations:

Example #1: Paper documents (such as purchase orders, obligations, modifications, receiving reports, invoices, correspondence, etc.) go through a scanner and become electronic images via the WINS interface. Next, the documents are indexed in the WINS system to allow the images to later be searched for specific items and retrieved. In indexing, important bits of information from the documents are manually entered into the system and associated with the images. After being scanned and indexed, the documents are routed by an imaging and distribution application within the WINS system to the appropriate accounting team for processing.

Example #2: Electronic documents (purchase orders, obligations, modifications, receiving reports, invoices, correspondence, etc.) are received and entered into the system, and images are rendered automatically. The electronic documents are also routed to the appropriate accounting operations team at the FINCEN for processing.

Financial transactions that occur in the Core Accounting Suite are consolidated and reported to the various departments of the federal government as required by law.

These systems throughout the remainder of the PIA will be referred to as the Core Accounting Suite.

Section 1.0 Information Collected and Maintained

1.1 What information is collected, used, disseminated, or maintained in the system?

The following information is contained within the Core Accounting Suite.

Individual Information

- Name (First, Middle, Last)
- Social Security Number (SSN)

- Date of Birth
- Mailing address including zip code (Business and personal)
- Telephone Number (Business and personal)
- Fax Number
- Email address (Business and personal)

Vendor Information

- Company Name
- Address
- Telephone Numbers
- Point of Contact
- Tax ID Number (TIN)
- DUNS Number (This is a unique, non-indicative 9-digit identifier issued and maintained by Dunn & Bradstreet that verifies the existence of a business entity globally – there is a separate DUNS number for each physical location.)
- Bank Account Number
- Bank Routing Number

Reimbursement Information

- Bank Account Number
- Bank Routing Number
- Credit Card Infromation
- FINCEN Account Number

Core Accounting System: The Core Accounting System contains sensitive but unclassified (SBU) information. Names, addresses, bank account numbers, and bank routing numbers of vendors and outstanding billing amounts for payment documents are examples of this SBU information. Information regarding proposals, bids, and payment and billing status for contracts is retained within the system.

Finance and Procurement Desktop (FPD): FPD contains sensitive but unclassified (SBU) information. Names and addresses of vendors, account numbers, SSN's, and purchase order documents are examples of this SBU information. Information regarding procurement requests, simplified acquisitions, receipt of goods/services, budgeting, and funds distribution are retained within the system.

Workflow Image Network System (WINS): The information is not necessarily collected but rather submitted by vendors or individuals for the payment of invoices and claims. This data may contain information such as vendor name, addresses, account number, social security number and tax identification number. WINS uses a wide variety of document types, and the, information submitted varies based on the document type.

The information is submitted by vendors or individuals for the payment of invoices and claims. The information submitted may contain information such as vendor name, addresses, account number, SSN, and tax identification number.

Representatives from vendors submitting invoices to the FINCEN provide contact information and other personal information as a representative of the vendor. Some of the documents processed by the system contain PII data for USCG personnel seeking reimbursement for travel.

An invoice from vendors will contain different information than a travel reimbursement claim from government personnel.

- For vendors, a vendor representative's name and contact information is required when processing the invoice in the Core Accounting System.
- For individual submissions, the name of the person, their contact information and identity verification information (such as SSN or supervisor's name and contact information) will be submitted via standardized forms for further processing in the Core Accounting System.

Sunflower Asset Management (SAM): Based upon the individual's role, the types of collected information that can be viewed via Sunflower include:

- Location Assignment
- Work Email Address
- Work Telephone Number.

Contract Information Management System (CIMS): The user profile information comes directly from FPD and the SSN is no longer captured when the user profile is created. In CIMS, there is a SSN column, but this field is not utilized. The only personnel with access to this field are those who have SQL backend access query capability. The SSN field is not visible at the application level. The SSN field is not a requirement for a user profile to be created within FPD/CIMS, and the field no longer exists at the application level when the user profile is created.

1.2 What are the sources of the information in the system?

A web server determines which applications the agencies' and users are permitted to access. Each agency has a separate web site from the other that allows them to access only their information. The main source for the Core Accounting Sub-System is the interaction with the FPD, and Sunflower application servers and the database tables stored on these servers. The main source of information for the Vendor Management System comes from Central Contractor Registration (CCR), the creation of vendor accounts via FPD, and an on site FINCEN team that creates vendor accounts via a vendor maintenance system. The USCG Marine Information for Safety and Law Enforcement (MISLE) system places information on an FTP server at USCG Operation Systems Center (OSC) that is subsequently pulled by FINCEN and placed into the Core Accounting System.

The FPD Sub-System is the enterprise-wide accounting and procurement sub-system used by USCG, TSA, and DNDO to create and manage simplified procurement documents and to maintain accurate accounting records agency wide. FPD is a mission critical application within FINCEN responsible for producing accurate and timely financial management information and related business reports, processing financial transactions effectively, executing fiduciary and stewardship responsibilities in consonance with policy and regulatory authorities, and establishing and maintaining accounting controls over USCG resources.

All basic procurement and accounting functions are centrally located in this application. This gives the USCG, TSA, and DNDO Procurement Shops the ability to electronically process their procurement needs and electronically route those request to the FINCEN for payment. The FPD Application is divided into seven sub modules, System Administration, Reports, Requisitions, Simplified Acquisitions, Receipt of Goods, Reconciliation and Budgeting and Funds Distribution.

Workflow Image Network System (WINS): This information is voluntarily supplied from commercial vendors and invoices, from individual member's claims for reimbursement, and from any other individuals or organizations requesting payments from the FINCEN. The main source of the information is from paper copies submitted from the field, but WINS also processes digital images that are sent via FTP from USCG units.

Sunflower Asset Management (SAM): All access to SAM is initiated via the Auto Access Request (AAR); FINCEN uses the documented AAR System to manage user identifiers. Once approval to the SAM system has been established, users are responsible for updating the profiles with the PII. Although PII information is captured during the single sign-on process via AAR, the information is not pushed to the SAM system, only the logon name.

Contract Information Management System (CIMS): The information is transmitted from FPD and is only stored at the table level. Initial purchase request information is transmitted from FPD to CIMS. Vendor information is entered into the vendor tables stored in CIMS by the Contracting Specialists and/or Contracting Officer.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected to support the FINCEN and other organizations with processing accounting and financial data.

- Vendor information such as company name, address, bank account numbers, bank routing numbers, telephone number, points of contacts, TIN number, and DUNS number are used to assist with processing financial queries.
- Information such as name, address, SSN, telephone number is collected for purposes of reimbursements for travel, etc.
- Information such as names, addresses and telephone numbers are used for debt collections, civil fines and penalties, user fees and payroll debt collections.

Reports are used for data selection or data filtering capabilities. The Reports applet allows a user to View, Print or E-Mail various formatted reports pertaining to accounting, budget, credit card transactions, funding information, procurement, receiving, reconciliation and system administration.

Requisitions allow system users the ability to create temporary additional duty orders, create procurement requests, enter record commitments, enter requisitions, obligations and approve requisition documents.

Simplified Acquisitions allow users to create various purchase documents such a credit card purchases, purchase orders (OF-347/SF-1449), miscellaneous documents, recurring charges, create amendment of solicitation/modification of contracts (SF-30), create Military Interdepartmental Purchase Requests (MIPR) and create Blanket Purchase Agreements.

Receipt of Goods captures and acknowledges a complete or partial receipt of goods. It also provides a means to produce Personal Property Accountability data on all line items, and a way to manually download the PPA data to magnetic media.

In the procurement sub-system information is collected within this application to identify transactions specific to a vendor and the capability to track the procurement to the initiating unit.

Information collected during image processing is being collected for the purpose of creating and writing payment transactions to commercial vendors and settlement of individual claims, for government travel account processing, for the creation of pay authorization allowance notifications, for household good moves, and for military member's incentive pay and tax withholding reporting on self-procured moves.

1.4 How is the information collected?

Information is collected by multiple subsystems via data exchange. The system does maintain PII information within its database tables. This PII collected is only recording vendor information that is entered from the user attaining the appropriate access privileges. The information is not collected but rather submitted by USCG Contracting Officers. These individuals provide their name and a telephone number where they can be contacted. The Core Accounting System collects information for financial processing from a General Ledger that pulls information from an Oracle Database Financial Module. Information such as SSN's, home addresses, bank account info, credit card info, and payroll records are processed. The information from the databases are processed in an automated fashion using API interfaces and stored in the Oracle Databases.

1.5 How will the information be checked for accuracy?

The Core Accounting Suite primarily receives data via manual data entry and as input (e.g., downloads) from other IT systems. The Suite implements discretionary access controls to prevent unauthorized access to and/or modification of data, which promotes integrity and accuracy of system data. To support the accuracy of data (e.g., data entry and transaction approvals), role-based access controls and a formal account management process ensures only authorized individuals are assigned permissions to perform authorized functions. This will minimize the risk of malicious or inadvertent modifications that affect the accuracy of data.

Financial and procurement data is verified and approved for submission into the system by finance and procurement staff managers, consistent with the Core Accounting System workflow approval process. The Core Accounting System checks data for accuracy based on system rules and edits, and verifies that data entered in certain fields exists in reference tables. In addition, to support data accuracy, financial management and procurement staff perform regular financial audits as part of their job functions; data integrity checks are performed via workflow structure, syntax and value checks. Audit log review is performed by the Core Accounting System support staff in accordance with Federal, DHS and the Core Accounting System Requirements.

In addition, information submitted to WINS is verified against information stored in the Finance and Procurement Desktop (FPD) and the Core Accounting System. WINS is strictly a feeder system which only assigns documents to financial management workflows which are executed in the Core Accounting System and FPD.

Information submitted to the SAM system is checked for accuracy based on a threshold level. As a control, if an asset that meets the capitalization threshold (greater or equal to 50K) is added to Sunflower, that particular asset will flow through the web services and reside in the Core Accounting System Fixed Assets (FA) Approval Inbox until approved by FINCEN personnel. Once FINCEN receives the proper documentation Government Property Information Sheet (GPIS), the asset data within the FA Approval Inbox will be verified with the GPIS and if all data is accurate, the asset will be approved. The asset will not actively reside in both SAM and the Core Accounting System FA and financially impact TSA set-of-books (depreciation). This control is mentioned because as part of the accuracy check, any captured PII will follow the record in the SAM system.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The authority for this agreement for the USCG is based on 31 U.S.C. § 1535, 1536.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Unintended or unauthorized disclosure of privacy information outside of those with a need to know.

Mitigation: To mitigate these potential risks, the Core Accounting Suite and hosting facility has implemented managerial, operational, and technical security controls consistent with DHS 4300A and associated information technology security standards, which are derived from National Institute of Standards and Technology (NIST) 800-53 *Recommended Security Controls for Federal Information Systems* to mitigate the identified risks.

Examples of managerial controls employed include, but are not limited to, performing certification and accreditation, developing and maintaining an up-to-date and approved system security plan, and performing risk assessments. Operational controls that have been implemented include security training

and awareness that cover an individual's security-related responsibilities, development of an incident response capability, media protection policy and procedures development and enforcement, and physical and environmental protections (e.g., guards, access badge security, sign-in logs, and security cameras).

Technical controls employed include implementing access controls (e.g., role-based access controls, account management procedures to include separation of duties, principle of least privilege, need-to-know, timely account disablement/deletion, and annual account recertification), defining, introducing, and enforcing identification and authentication mechanisms; and creating system protections to include encryption of information at rest and in transit and boundary protection technology and procedures (e.g., network intrusion detection systems, firewall log monitoring, and malware detection and correction software).

To prevent unauthorized data use by agency employees, access control audit log reviews are performed by FINCEN personnel in accordance to DHS and Federal requirements. All DHS employees and contractors who have access to privacy information are required by law and by contract to protect personal information in accordance with the Privacy Act and DHS privacy guidelines. Unauthorized use by a Federal employee is subject to strict penalties. Policies and procedures are in place and/or being developed that cover the Core Accounting System user responsibilities (e.g., handling of information and need-to-know).

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

FINCEN uses the Core Accounting Suite to process all of the daily financial transactions. The respective finance staffs are responsible for the accounting programs, which include supporting the process of funds flowing to, from, and within the USCG and other DHS clients, providing accounting services for all employees, and supervising the accounting policies, standards, systems, and activities.

The Core Accounting Suite records consist of financial and procurement data, to include all documents used to reserve, obligate, process, and affect collection or payment of funds, invoices, purchase orders, travel advances and travel/transfer vouchers. In addition, it is used to establish payments due or made, claims, or debts owed by the individuals working or doing business with the USCG. This includes fees, fines, penalties, overpayments, and other assessments.

The Core Accounting Suite collects procurement information to allow for the prompt and proper payment of entities providing goods and services to the USCG, TSA, and DNDO. It uses procurement information to produce accurate and timely financial management information and related business reports, process financial transactions effectively, execute fiduciary and stewardship responsibilities as it applies to policy and regulatory authorities, and to establish and maintain accounting controls over USCG resources.

Core Accounting Suite also uses information to provide primary business functions for asset management such as purchase orders, contracts, acquisitions, transfers, retirements, modifications, and asset tracking for TSA.

Finally, USCG and TSA utilize information for formal contract creation and management, including milestone planning, solicitations, award, and closeout.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The Core Accounting Suite currently does not use tools to analyze data. There are, however, several reports that are made available to active users based upon their respective roles. These reports are not known to be distributed to internal or external entities for specific or required purposes. The CAS Suite is a transactional based system not an analytical based system.

Workflow Image Network System (WINS): WINS does not utilize any kind of data mining utilities to generate additional information or data. Data submitted to WINS is used "downstream" in the financial management process to process reimbursements and payments. Data elements are used to verify that payments are made to the correct person or organization. Data is submitted via Coast Guard approved forms.

Sunflower Asset Management (SAM): No tools are used within the SAM system to analyze data. However, as a system feature, several reports are available to active users based upon their respective roles. These reports are not known to be distributed to internal or external entities for specific or required purposes.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy Risks: Unintended or unauthorized disclosure of privacy information outside of those with a need to know.

Mitigation: Core Accounting Suite is undergoing its first certification and accreditation. Security controls associated with confidentiality, integrity, and availability are tested as part of the Security Test and Evaluation Assessment process based on the security control requirements articulated in NIST SP 800-53.

Security controls associated with access, data integrity, and data retention are tested as part of the Annual Self-Assessment process based on the security control requirements articulated in NIST SP 800-53.

Access controls are employed to ensure that only authorized, trained users have access to the system to conduct their prescribed responsibilities. Core Accounting Suite is categorized as a moderate system in accordance with the FIPS-199 System Security Categorization worksheet. Security controls associated with access, data integrity, and data retention are tested as part of the Annual Self-Assessment process based on the security control requirements articulated in NIST SP 800-53.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The information in Core Accounting Suite is retained indefinitely. The information has been retained in the databases since the initial subsystems obtained operational status in 1996, and is being retained for the life span of the database.

FINCEN destroys the information collected when the purpose for which it was provided has been fulfilled unless it is required to be kept it longer by statute or official policy.

Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules approved by the National Archives and Records Administration. The prescribed period of retention is six years and three months. However, in some cases information submitted to the USCG may become an agency record and therefore might be subject to a Freedom of Information Act request.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The information is required to be maintained for six years and three months as it relates to financial payment information for USCG product, service providers, and NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk identified was the potential for reaching maximum storage capacity for the total volume of records accumulated by the system. Additional servers and storage arrays have been procured to address any potential problems associated with the secure storage of the data.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Core Accounting Suite contains sensitive but unclassified information. Information regarding proposals, bids, and payment and billing status for contracts is retained within the system.

System interconnection is the direct connection of systems for the purpose of sharing information resources. Internal interconnected systems communicate via the FINCEN Local Area Network (LAN). All these systems reside on the FINCEN side of the firewall, not directly connected to CGDN+. Web services are based on XML code and sets procedures that pass information from one set of tables in a database to tables in another based on coded rules.

The WINS sub-system privacy information is only shared with the USCG Personnel Service Center (PSC). Incentive payment and tax withholding amounts are reported to PSC by member SSN for the purposes of W-2 income and tax reporting.

The SAM sub-system privacy information such as, vendor information including company name, company address, telephone numbers, Tax ID numbers, are only shared with TSA and potentially DHS via canned reports.

The CIMS sub-system privacy information is not shared with any other agency.

The FPD sub-system privacy information is not shared with any other agency.

4.2 How is the information transmitted or disclosed?

Internal information is transmitted via CGDN+. PII is disclosed only to authorized users with the need-to-know.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: Unintended or unauthorized disclosure of privacy information outside of those with a need to know.

Mitigation: From an information technology perspective, privacy risks may result from a breach to the Core Accounting Suite security posture, which could subsequently compromise the confidentiality, integrity, and availability of information. If a breach were to occur, primarily via unauthorized access to or use of PII, it would provide an unauthorized individual the opportunity to examine, collect, alter and/or

otherwise misuse the information. In addition, if PII data is altered, integrity may be lost, resulting in fraud and abuse

Internal sharing risks also include unauthorized staff or personnel obtaining the ability to view or modify information within Core Accounting Suite. Hard and soft-copy media may be misplaced or used inappropriately within the Core Accounting Suite Program.

Unauthorized physical access to Core Accounting Suite data within the hosting facility is prevented through the use of guards, access badge security, and sign-in logs, as well as via the implementation of policies and procedures that describe access requirements. Unauthorized logical access to the Core Accounting Suite itself is addressed by log monitoring, and malware detection and correction software.

Data is protected through compliance with DHS access control policy, role-based access control for user identification/authentication, assigning and enforcing authorizations, establishing thresholds, applying information flow restrictions, automated system notifications, session termination, and applying the principles of least privilege coupled with a need-to-know.

Core Accounting Suite has established and implemented an account management process to include account justification, requirement of a background investigation and clearance, access restrictions based upon separation of duties and least privilege, strong authenticator management, certification efforts, and audit management.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared, and for what purpose?

Core Accounting Suite privacy information is shared with the following external organizations for financial transactions to take place to support the services within the Core Accounting System and its supported applications.

Financial Data exchanges are conducted with exchange financial data with DNDO for payments; financial accounting data is transmitted from FINCEN to the USCG Treasury for daily payment information. Data is copied onto floppy disk and carried to the Financial Management System to be sent via the Connect Direct software application over a leased line to the FMS network. IRS 1099 forms are sent to IRS, Budget Execution Data System Reports are sent to the Office of financial systems, Daily payment data, Debt referral transactions, contract project data, and General Ledger consolidated data is sent via the Core Accounting Suite.

The Consolidated Billing System batches and Data Extracts are sent externally to Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and

Customs Enforcement (ICE), and U.S. Secret Service (USSS). FINCEN sends files to USSS via a dedicated link on the DHS CGDN+ for purchase card transactions.

Electronic Data Interchange (EDI) transactions are conducted with via General Transactions (GENTRAN) which reads, translates and maintains EDI data and information on Windows & UNIX platforms.

A Transfer of all Fund Code tables from MPS to the OSC is conducted to keep the ARMS Fund Code tables in sync with the FINCEN funding code tables.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. All sharing of information is covered by routine uses in the Department of Homeland Security Accounts Payable System of Records DHS/ALL-007 (October 17, 2008, 73FR 61880), Department of Homeland Security Accounts Receivable System of Records DHS/ALL-008 (October 17, 2008, 73 FR 61885), and the Department of Homeland Security Asset Management Records DHS/ALL-010 (October 23, 2008, 73 FR 63181) SORNs.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The methods of information sharing are via FTP and S/FTP (file transfers), email attachments, batch processes, web-based applications, PKI Certificates, the USCG Messaging System and the CGDN+.

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: Privacy risks include inappropriate disclosure of sensitive information to include unauthorized individuals who do not have a need-to-know as well as unauthorized disclosure in the transmission/exchange of information.

Mitigation: Privacy risks are mitigated through the implementation of mechanisms that are described in data sharing agreements such as Memorandum of Understandings (MOUs) and/or Interconnection Security Agreements (ISAs), which describe how each Component must address information exchange security, trusted behavior expectations, incident reporting, auditing, and security parameters of both the Core Accounting Suite and external organization.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

All of the forms are USCG approved forms and were developed to include the appropriate privacy related statements which include why the information is required and how it will be used. Additionally, notice is provided in pursuant with 5 U.S.C. §552a in the Department of Homeland Security Accounts Payable System of Records DHS/ALL-007 (October 17, 2008, 73FR 61880), Department of Homeland Security Accounts Receivable System of Records DHS/ALL-008 (October 17, 2008, 73 FR 61885), and the Department of Homeland Security Asset Management Records DHS/ALL-010 (October 23, 2008, 73 FR 63181).

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Individuals and vendors are required to submit this information in order to receive payment or reimbursement. If individuals or vendors do not wish payment or reimbursement, they do not have to complete claim forms and submit information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

When individuals or organizations complete the required forms for requesting reimbursement or payment, they are authorizing the use of this information to facilitate the efficient disposition of their claim or request.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Unintended or unauthorized disclosure of privacy information outside of those with a need to know.

Mitigation: Information is submitted to the system for financial reimbursements. Users must click through an acknowledgement screen stating they understand they are using a federal information system and are only authorized to access the system for official purposes.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Core Accounting Suite users are required to review and sign the Rules of Behavior before being granted access to the system. All users are required to complete annual Information System Security training and provide a signature documenting their understanding prior to assignment of USERID and password.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

USCG FOIA Coordinator

2100 2nd Street, S.W.

Washington, D.C. 20593-0001

Individuals may also submit requests by fax at 202-475-3522 or by email at efoia@dhs.gov. If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

Note: AAR/SSO maintains controls for access to the Core Accounting Suites.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an error in the users access profile is discovered, the first line of action is to contact the UMS helpdesk. The helpdesk will record a Trackit Issue and review the PII for accuracy. If found to be inaccurate, depending on the outcome, the trouble ticket will be routed to the appropriate areas for correction.

Erroneous information can only be discovered in the event that a payment is made to the wrong entity or that payment has not been received. In either potential case, individuals are instructed to contact the customer service center, which will initiate steps to validate or update individual information.

7.3 How are individuals notified of the procedures for correcting their information?

Information is provided on the FINCEN Internet homepage which is provided to vendors working with the USCG and to all USCG units.

7.4 If no formal redress is provided, what alternatives are available to the individual?

No redress is provided via Core Accounting Suite, but alternatives exist in that individuals are instructed to contact the customer service center which can resolve issues of misinformation with the appropriate system of record.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No redress is provided via Core Accounting Suite but alternatives exist in that individuals are instructed to contact the customer service center which can resolve issues of misinformation with the appropriate system of record.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

User account requests are handled by an automated web site. This site contains the information of the user requesting access as well as their supervisor's information to validate the request. Personnel requesting info must have a valid email account and access is granted based on roles and responsibilities. The procedures of determining the appropriate role to be given to users is documented and maintained by the FINCEN Information Systems Division.

8.2 Will Department contractors have access to the system?

Yes contractors will have access to the system, to include DHS and USCG contractors.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Users and each new FINCEN employee must complete the USCG's general mandated Privacy Awareness training and FINCEN's information system (AIS) security brief annually.

FINANCE CENTER STAFF INSTRUCTION 5260.1 specifically addresses Privacy and PII. The instruction provides FINCEN's policy for managing inquiries regarding personal privacy information, protecting privacy information, reporting privacy incidents and training FINCEN personnel regarding privacy issues. The instruction affects all FINCEN personnel.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Core Accounting Suite is undergoing its initial certification and accreditation.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

End-user behavior is dictated in the system by use of roles and permissions. Tight access controls are employed in the granting of user accounts. Supervisors must approve a proposed user's need to know and the application owners must approve the requested access. The content of the roles are audited on a regular basis to insure that an end-user cannot gain inappropriate access to the system.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risks identified are associated with inaccurate entry of information. Data checking logic and dependency on other applications were identified as sufficient to address data integrity issues. Invalid entries are flagged and rejected prior to permanent posting to the system. Access controls identified as in place and effective during the C&A process also validated that only trained personnel have access to the system for completing specific accounting functions.

Section 9.0 Technology

9.1 What type of project is the program or system?

Core Accounting Suite is a CFO designated financial system.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Core Accounting Suite is in the development phase of the systems lifecycle. The suite was developed to accurately reflect the boundaries as defined in the OMB Exhibit 300 submission.

Currently, the Core Accounting System, Finance Procurement Desktop, and WINS are identified as separate systems in Trusted Agent (TA) and are in the operational phase of the system lifecycle management. However, upon completion of the Core Accounting Suite certification and accreditation process, the existing systems will be removed from inventory as separate systems and identified as subsystems within the Core Accounting Suite. In addition, CIMS and Sunflower will be added to the DHS inventory as subsystems to the Core Accounting Suite.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Not Applicable.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security