Privacy Impact Assessment
for the

Electronic Contract Filing System (ECFS)

DHS/ALL/PIA-065

June 7, 2018

Contact Point
Brian Wilson
Oversight and Strategic Support/Acquisition Systems Branch
Office of the Chief Procurement Officer
(202) 447-0904

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Management Directorate, Office of the Chief Procurement Officer (OCPO) has developed the Electronic Contract Filing System (ECFS). ECFS functions as a contract storage system throughout the lifecycle of a contract, and will be the authoritative source of the contract file in an electronic format for DHS Components as the Department moves away from paper-based management. In addition to contract file storage, ECFS supports workflow, document management, and records management. DHS is completing this Privacy Impact Assessment (PIA) because ECFS stores personally identifiable information (PII) on DHS personnel and vendor contacts.

Overview

The Department of Homeland Security (DHS) Office of the Chief Procurement Officer (OCPO) is responsible for awarding and administering contracts and purchase orders to support the DHS mission, goals, and objectives. OCPO provides vital procurement and logistics services to DHS Components, support offices, and leadership in applying fundamentally sound business practices to the Department's acquisition of goods and services. The use of paper-based processes across the Department hampers its mission because staff do not have easy access to documents required to perform their work. Furthermore, as the Department embraces remote working trends, disaster preparedness, and improved operations, paper-based processes do not allow contracting staff to efficiently work on files that cannot be accessed remotely. To resolve these issues, OCPO has developed the Electronic Contract Filing System (ECFS), which will act as a digital storage cabinet to store final contract artifacts, allowing users to efficiently search for them rather than thumbing through paper documents.[1]

ECFS is a commercial off the shelf (COTS) product, provided by the company AINS, that will use a Federal Risk and Authorization Management Program (FedRAMP)-approved cloud-based solution. AINS's case management platform, eCase, is a complete and automated information management, tracking, and reporting solution. eCase provides a means of controlled collaboration and oversight between multiple users, simultaneously allowing for increased productivity while decreasing human error. eCase can be deployed enterprise-wide so that users from multiple offices and scattered locations can collaborate at whatever respective level of input is required, from an approval signature to a grammar correction within a document. ECFS uses the AINS eCase case management platform for electronic archiving of procurement documents

[1] Contract decisions and awards will continue to be made through the applicable contract writing system, such as the Procurement Request Information System Management (PRISM). ECFS is a reference point; a user may refer to a market research report document that has been stored in ECFS for questions about potential businesses that can meet a requirement, but ECFS is not a facilitator for awarding a contract. For more information about PRISM and its use of DHS contract data, please *see* DHS/ALL/PIA-013 Procurement Request Information System Management (PRISM), *available at* https://www.dhs.gov/privacy.

Department-wide.

Contracting officers and contract specialists will be able to create digital contract files in which they can store all of the phases of a contract, from Pre-Solicitation to Contract Closeout. The files can be uploaded from ECFS users' hard drives and shared drives. If required, users may choose to scan paper documents and then upload the digital copies, but ECFS will be a "point-forward" system in which brand new purchase requests will be stored in ECFS.[2] ECFS will store the data throughout the active lifecycle of the contract. Once the contract file has been closed and final payment made, the Records Manager will then designate the file for archiving. ECFS will then retain a digital copy of the contract file and metadata for six (6) years. Once that retention time has been met, the Records Manager will go through a manual process to "destroy" the file.

ECFS allows for users to create a number of contract-related reports, to include:

- Contracts assigned to a user;
- Contracts assigned to a Component/office; and
- Contracts by phase (*i.e.*, Pre-Solicitation, Solicitation, Pre-Award, Award, Contract Administration, Contract Closeout).

ECFS also allows for the creation of a number of audit reports, to include:

- User login data (date, time, how long users were logged in); and
- User account report (user ID, office code, etc.).

The information collected by ECFS consists of data elements about DHS authorized users and vendor contacts. The information ECFS collects about DHS authorized users includes: name, email address, office code, phone number, SAMaccountname,[3] tasks assigned to a particular user, contracts that were created by a user, and login reports for when a user logged into ECFS, and the duration of that particular session.

Only authorized DHS personnel have access to ECFS. The information ECFS collects on these individuals only includes basic contact information for workflow accountability, general communication, and login purposes.

The information ECFS collects from vendors contains contact information, as well as Requests for Information (RFI)/Request for Proposals (RFP)/Request for Quotes (RFQ); market research reports; vendor proposals, bids, and financial information; and Acquisition Plans and Purchase Request documentation.

[2] Current paper files will not be scanned and loaded into ECFS. Those files will continue to be managed physically until they are closed and archived.

[3] SAMaccountname is the user's Windows naming attribute that is required for Single-Sign On access to ECFS. Every DHS user has a unique SAMaccountname (over the whole domain). This attribute is needed for users to be able to log in using Single-Sign On instead of username and password.

The eCase system has multiple layers of security that protect content to the object level and can be applied to a user, group of users, or set as a general feature. Account access within the system is also limited in that users have a defined time period during which their access is active. This automatic feature will log out inactive users and disable their user account based on their access needs. The system can generate both usage and customized access reports that will report users who have been inactive or disabled from the system as needed.

Additionally, the audit trail feature, unique identification, authentication requirements, and mandatory security, privacy, and records training requirements help prevent unauthorized access to data, browsing, and misuse.

OCPO is currently developing the ECFS System Security Plan (SSP), while the AINS eCase application SPP has already been created. AINS provides and manages the software through a FedRAMP-compliant cloud hosting location, which delivers a standard approach to security assessment, authorization, and continuous monitoring for the Federal Government. The AINS eCase ECFS software application is isolated from any other applications in the hosting location. AINS, the software contractor, has provided documentation to the ECFS Information System Security Officer (ISSO) that confirms ECFS servers are logically separated from the rest of the AINS environment. AINS provides monthly scans as part of the contract service to the ECFS ISSO, who validates the security scans and performs continuous monitoring to ensure compliance with the implementation of security controls identified in the DHS 4300A Sensitive Systems Handbook,[4] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, and NIST SP 800-53.

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?

A number of legal authorities require the recordkeeping of procurement-related documentation. Those authorities include:

- OMB M-12-18, Managing Government Records Directive (August 24, 2012);
- Federal Acquisition Regulation (FAR), 48 C.F.R. §§ 1-53;
- Homeland Security Act of 2002, Pub. L. 107-296, 116 stat 2135 (November 25, 2002); and
- DoD 5015.2 Retention of Contractor Records.[5]

[4] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

[5] This is the records management authority that DHS follows. DHS does not have its own Department-wide standard, and NARA accepts this Department of Defense (DoD) standard.

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

Vendor information collected, maintained, and used by ECFS is covered by DHS/ALL-021 Department of Homeland Security Contractors and Consultants.[6] DHS personnel information collected for the purposes of access to the system is covered by DHS/ALL-004 General Information Technology Access Account Records System.[7]

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

The ECFS System Security Plan is currently being developed. The ECFS Authority to Operate (ATO) is expected to be granted in May 2018, following completion of this PIA. The AINS eCase application COTS product that forms the basis of ECFS is operating under a FedRAMP ATO granted in 2017. A FedRAMP System Security Plan has been completed for AINS eCase.

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

Retention periods of data for contract information vary according to context and circumstance, but, with respect to completed contract files, disposal customarily occurs six (6) years after final payment. ECFS will archive and store closed contract files in accordance with the DHS Retention Schedule reflected in National Archives and Records Administration (NARA) General Records Schedule (GRS) 1.1, Item 10 - Financial Management and Reporting Records.[8]

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.

ECFS does not collect information directly from external sources or the public, nor are there any forms that are accompanied with documents that are uploaded into ECFS for final storage. The Paperwork Reduction Act (PRA) is outside the scope of ECFS, as the PRA is applicable during the standard procurement and contract process prior to ECFS. ECFS is simply a document repository and records management solution.

[6] DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179 (October 23, 2008).
[7] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[8] *See* https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf.

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.

The information collected by ECFS consists of data elements about DHS authorized users, vendor contacts, and procurement-sensitive information.

Information maintained in the system for DHS authorized personnel is limited to the following:

- Full name;
- SAMaccountname;
- Office code;
- Work telephone number; and
- Work email address.

ECFS also able to collect information on tasks assigned to a particular user, contracts that were created by a user, and login reports for when a user logged into ECFS and the duration of that particular session.

Information maintained in the system for vendors is limited to the following:

- Vendor contact full name;
- Vendor contact work telephone number;
- Vendor contact work email address and websites;
- Vendor address; and
- If necessary, full names of key personnel in a vendor proposal.

Information maintained in the system related to procurement-sensitive information includes the following:

- Requests for Information (RFI), Requests for Proposals (RFP), and Requests for Quotes (RFQ);
- Market research reports;
- Vendor proposals, resumes for key vendor personnel, bids, and financial information (vendor labor rates and product pricing); and

- Acquisition Plans and Purchase Request documentation.

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

ECFS is a standalone solution with no integration to PRISM[9] or any other contract writing system. ECFS is web-based and users go to an Internet URL for system access. Users at the different DHS Components will upload or download digital procurement documents from or into ECFS. ECFS users will be uploading documents into ECFS for final storage within their digital contract files. The documents originate from the user's hard drive, shared drives, SharePoint, and the contract writing system.

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

ECFS does not have an electronic interface with any external sources for public data, but users may manually enter information about vendors from public sources such as vendor name, address, phone numbers, and website.

2.4 Discuss how accuracy of the data is ensured.

The eCase product includes various syntax checks to ensure the accuracy of the data entered into ECFS. These syntax checks include character set, length, and numerical range to verify that acceptable values are in place to ensure that fields are properly entered. In addition, some fields are required to be completed prior to submitting a query to the database. If these fields are incomplete, the data is not passed through to the database.

The application itself has many other fields that have validity checks. For example, a user cannot enter anything but the date in a date field. Hierarchy constraints exist that limit the user from selecting certain items in the drop-down lists until the prior drop-down list has been selected. Lastly, a user cannot be deleted from the system if he/she created or worked on a previous case. The user may be marked as inactive,[10] and unable to access the system, but cannot be deleted because that would delete the case data. Error messages generated by the eCase system provide timely and useful information without revealing potentially harmful information.

Additionally, the OCPO/Acquisition Systems Branch (ASB) has contracted with an Independent Verification and Validation (IV&V) organization to test the quality and accuracy of data associated with systems associated with OCPO/ASB, including ECFS. A test system is being

[9] *See* DHS/ALL/PIA-013 Procurement Request Information System Management (PRISM), *available at* https://www.dhs.gov/privacy.

[10] Component "super users" or System Administrators will manually mark users as inactive based on personnel leaving changing offices, no longer have a need-to-know, or leaving DHS.

established by the IV&V contractor to evaluate the quality and accuracy of ASB system data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of unauthorized access to vendor and procurement-sensitive information.

Mitigation: ECFS is not a public-facing system. Only DHS personnel authorized to use the system will be granted access. Users who have had their accounts marked as inactive will no longer have access to the system and its data. Additionally, ECFS has multiple layers of security that are applied to a user or group of users. The audit trail feature, unique identification, authentication requirements, and mandatory security, privacy, and records training requirements also help prevent unauthorized access to the data.

Privacy Risk: There is a risk of over-collection of information with information being stored in paper files and digitally in ECFS.

Mitigation: OCPO will conduct continuous education to users informing them that ECFS is the official source of contract files and that they no longer to need to create new paper files and binders. The policy and instructions for ECFS will be added to the Homeland Security Acquisition Manual (HSAM).[11]

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.

The information collected by ECFS consists of data elements about DHS authorized users, vendor contacts, and procurement-sensitive information. The collection of vendor information is necessary for basic identification of vendors that are in the process or have received the award of a DHS contract.

ECFS will act as a digital storage cabinet to store final contract artifacts. No final contract decisions or awards will be made based on the information within ECFS. Those decisions will continue to be made through the applicable contract writing system. ECFS is simply a storage capability that will allow users to generate reports with the information.

In direct compliance with OMB Memorandum M-12-18, *Managing Government Records Directive*,[12] DHS requires that all files be stored in an electronic format. Part I, 1.1, states that, *"By 2019, Federal agencies will manage all permanent electronic records in an electronic format."* Additionally, ECFS supports DHS's disaster preparedness and continuity of operations initiatives

[11] *See* https://www.dhs.gov/publication/hsam.
[12] *See* https://www.archives.gov/records-mgmt/prmd.html.

by now storing all contract files in an electronic format, moving away from using filing rooms, cabinets, and personal binders.

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. While there is a query search function in the system to look up information, ECFS does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

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

Yes. DHS Components will have users with assigned roles and responsibilities in the system. However, they will not share procurement data with one another. ECFS is set up to only allow users who have been added to a particular contract file to see the content of that file. Each Component will have a "super user" that will provide Tier 1 support and will be able to view files for only his or her Component. For example, a U.S. Customs and Border Protection (CBP) ECFS Administrator will be able to view and troubleshoot all CBP-only files. However, he or she will not be able to access Transportation Security Administration (TSA) files. OCPO is the system owner and application administrator; as such, OCPO will be able to manage permissions and view files across the Department.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information contained within ECFS will be used for an unauthorized purpose.

Mitigation: This risk is mitigated by several factors built in to ECFS. All users have their own logins through Single Sign-On and they do not share user accounts to access the eCase application. User accounts are established and administered in accordance with a role-based access scheme that organizes all end user and privileged user accesses into roles. The application also does not use share groups; all the groups created within the application include users with the same type of permissions.

ECFS also has a built-in audit tracking capability that monitors the system accounts and their access and actions. All the actions done by the user are tracked. Reports can be generated in different formats in the application audit tool.

Users with privileged accounts are specifically authorized prior to the establishment of the account. Each privileged account user also maintains a regular user account for non-privileged access. This ensures privileged functions are properly audited.

In order to access ECFS, users will go to an Internet URL, accessed either through DHS's internal network or via the DHS virtual private network (VPN). If accessing via the VPN, access is only permissible through a set of IP ranges provided by network personnel. Unless the user has a pre-existing VPN account, he or she cannot access the application remotely. The firewall is used to monitor for unauthorized remote access to the application. If any inappropriate actions are discovered, an investigation will be conducted and the appropriate sanctions will be applied.

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.

ECFS does not collect a user's information without his or her knowledge or consent. The collection of information from a DHS-authorized user is not made prior to him or her completing an ECFS user account request and Rules of Behavior. Notice is also provided to employees by DHS/ALL-004 General Information Technology Access Account Records System. Upon logging into ECFS, the user will receive the following prompt: "You are about to access a U.S. Government information system; system usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and use of the system indicates consent to monitoring and recording."

ECFS collects information provided as existing documentation submitted during the procurement process. This information is provided voluntarily by vendors in response to RFPs, RFIs, and RFQs. The individuals may not know that the information they submit is stored specifically in ECFS, but will have some understanding that DHS is storing the information as part of the procurement process.

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

DHS personnel are requested to provide basic information, such as name, work phone, and work email address, for ECFS system access. An individual may decline to provide information; however, if certain basic information is not provided, the employee cannot be granted access to the system.

Vendors may elect not to submit their information to DHS as part of the procurement process in the first place. However, once the information is submitted, DHS uses the information in accordance with the FAR and other procurement/contracting authorities.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that vendors may not know their information is being stored in ECFS and how it is being used.

Mitigation: This risk is mitigated by several factors. Vendors know that submission of their information is voluntary. All of the required information is outlined in RFPs and other related documentation. While vendors may not know their information is contained specifically in ECFS, they will know that DHS is using the information in the procurement lifecycle.

This PIA provides additional notice of what ECFS is and how vendor information is being used and stored.

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.

ECFS user accounts are retained for the life of the system. Users who no longer require an account cannot be deleted from the system; however, the login rights are removed from the account and it is then deactivated. Deletion of user accounts would eliminate pertinent historical elements of the procurement records.

Retention periods of data for contract information vary according to context and circumstance. However, with respect to completed contract files, disposal customarily occurs six (6) years after final payment. ECFS will archive and store closed contract files in accordance with the DHS Retention Schedule reflected in NARA GRS 1.1, Item 10 - Financial Management and Reporting Records.[13]

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that DHS may maintain vendor and procurement-related information for longer than is required.

Mitigation: ECFS allows for the Records Manager to run a report on contract files that have met the 6-year retention period. From there, the Records Manager can "destroy" the file per NARA records management guidance. The System Owner will also perform yearly audits and reports to identify content that has exceeded the archival and records management retention period.

[13] *See* https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf.

Section 6.0 Information Sharing

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

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

The information within ECFS may need to be shared outside of DHS pursuant to a Freedom of Information Act (FOIA) request. Aside from that, the data about contracts, and not the documents themselves, would be obtained through other systems such as the contract writing system or Federal Procurement Data System (FPDS).[14]

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

Information in ECFS is not shared outside of DHS.

6.3 Does the project place limitations on re-dissemination?

No. Information in ECFS is not shared outside of DHS.

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

Information in ECFS is not shared outside of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no risks related to external information sharing as ECFS does not share personally identifiable information (PII) with external entities.

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?

Vendors do not have access to their information within ECFS. If they require access to

[14] The Federal Procurement Data System (FPDS) is a publicly available database that contains procurement transaction information. For more information, please *see* https://www.gsa.gov/tools/supply-procurement-etools/federal-procurement-data-system.

information about their proposal or other procurement-related data they should make that request outside of ECFS through their Contracting Officer.

U.S. citizens, Lawful Permanent Residents, or persons covered by the Judicial Redress Act, may also submit a Privacy Act (PA) request to access their PII. Requests for PA-protected information must be made in writing, and clearly marked as a "Privacy Act Request." The name of the requester, the nature of the records sought, and the required verification of identity must be clearly indicated.

Additionally, all individuals, regardless of citizenship, may seek access to the records by submitting a FOIA request. FOIA requests must be made in writing, and clearly marked as a "FOIA Request". The name of the requester, and the nature of the records sought must be clearly indicated.

Individual ECFS users are able to view their own profile information within ECFS and can run reports about their workload (*e.g.*, number of tasks assigned to them). However, they do not have access to change their own profile information or access permissions. That must be done through the ECFS System Administrator (*i.e.*, OCPO) or Component "super user."

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

ECFS is an electronic archive of DHS procurement files. Vendor information that requires correction would be required to be made through the respective contract writing system or the DHS Components that own the data.

DHS personnel with ECFS access are provided with procedures for making changes to their profile data. However, only system administrators can change settings for system ID or username in the ECFS system.

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

Vendors are not made directly aware of redress procedures for their information in ECFS other than through this PIA. However, vendors will know to correct any information through the formal procurement channels, pursuant to the FAR.

Individual users are made aware of how to correct their information within ECFS through the ECFS user account request process, or through other ECFS supporting documentation, such as the ECFS administration manual.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that a vendor may not be provided redress opportunities for their information in ECFS.

Mitigation: ECFS is unable to mitigate this risk itself. ECFS is an electronic archive of

DHS procurement files. Redress is provided by contacting the respective contract writing system or the DHS Components that own the data.

ECFS is only able to provide notice of this process through this PIA. However, the risk to inaccurate information within the system about a vendor is minimal because no final contract decisions or awards will be made based on the information within ECFS. Those decisions will continue to be made through the applicable contract writing system.

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?

The ECFS ISSO reviews audit logs on a weekly basis. The system provides full audit trail capabilities that automatically captures any action performed on the system, who performed the action, and when it was performed (date/time). All logon attempts are audited within the solution with date/time and workstation IP address information. The ECFS ISSO looks for unusual activities that might indicate misuse of the system. If such activities are discovered, the ECFS ISSO follows the security incident response procedures provided by the DHS 4300A Sensitive Systems Handbook.[15] The AINS Technical Manager also reviews audit information on a weekly basis for inappropriate or unusual activity. If suspicious activity is identified, the AINS system administrator and AINS Technical Manager perform additional analysis to determine what is actually occurring. Additional auditing will take place to further track the potential issue.

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

With all new users, the control of individual access to ECFS is enhanced through the use of automated Rules of Behavior, which includes a list of policies and procedures that users acknowledge in writing prior to gaining an ECFS account. The Rules of Behavior are displayed electronically to all new users prior to initial login and annually thereafter. Users must agree to abide by the Rules of Behavior prior to logging in. If they do not agree, the system will not permit them to log in.

Users of ECFS receive formal training. A training manual is used to guide the training sessions. Training covers the operation of the system from the users prospective and is interactive. The ECFS ISSO provides additional training for personnel when there is a significant change in ECFS's security environment, its security requirements, or when an employee's security role changes. AINS has developed a comprehensive computer security handbook that includes an

[15] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

overarching organization-wide information security policy and associated procedures.

Additionally, all DHS personnel are required to complete annual privacy and security 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?

User accounts are created based on applicable user groups within the application. The user is assigned to one of these groups and inherits the permissions associated with that group. All account creation takes place after the system administrator or AINS Technical Manager receive an account request form from the individual's supervisor. This request outlines the user's name, contact information, desired level of access, and manager's approving signature authorizing the account to be established. The system administrator then establishes an account for the individual and notifies them of the initial, temporary password to log into the application.

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?

OCPO/ASB will be completing Service Level Agreements with the Component users of ECFS that define the business relationship between the parties. There will be no agreements related to information sharing between internal DHS components or any entities external to DHS.

Responsible Officials

Brian A. Wilson
IT Project Manager, ECFS System Owner
Office of the Chief Procurement Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security