Privacy Impact Assessment
for the

Document Management and Records Tracking System (DMARTS)

September 8, 2008

Contact Point
Pamela J. Carcirieri
Deputy Director for Privacy
Records Management Division
Federal Emergency Management Agency

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Federal Emergency Management Agency (FEMA), a component of the Department of Homeland Security (DHS), has developed the Document Management and Records Tracking System (DMARTS). DMARTS is an Enterprise Content Management (ECM) system that collects personally identifiable information (PII) from claimants to carry out its mission of assisting individuals who apply for disaster assistance benefits. DMARTS will move paper files to an electronic repository. This PIA examines the privacy implications to ensure that adequate privacy considerations and protections have been applied to this electronic framework.

Overview

DMARTS is a component of FEMA's National Emergency Management Information System (NEMIS), an agency-wide system that provides a technology base to FEMA and its partners. DMARTS supports NEMIS by providing document capture, repository, and workflow functions. DMARTS will house data collected as the result of disaster assistance applications from individuals affected by Nationally Declared Disasters. DMARTS will not alter the data elements currently covered by the existing system of records and applicable paper applications that will now use DMARTS as a repository.

DMARTS is an assistance application receipt platform that collects PII from individuals, states, and/or agencies applying for disaster assistance benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, herein after referred to as "registrants". Information collected by DMARTS, to include the registrant's SSN, allows FEMA to positively identify registrants requesting Federal assistance. The collection of PII from registrants is essential to maintain up-to-date information on individuals to expedite application processing and render assistance in a timely and efficient manner.

A registrant applying for assistance is required to submit an application via telephone, or internet. Registrants may submit additional information in support of their application for assistance via fax or mail. FEMA employees or contractors enter information into DMARTS via three methods; fax servers, a contractor upload module, and scanning.

Once FEMA has a completed registration, data is moved to the FEMA Operational Data Store (ODS). The ODS is a central repository for FEMA NEMIS registration information. Information from the ODS is made available to the DMARTS application to allow the DMARTS user to identify the registrant that mailed or faxed a document to be added to their application. The DMARTS user retrieves the image(s) through analysis of pertinent data in the image, performs a query to locate the registrant's data. Once located, the indexer will add additional pieces of data, labeled Meta Data, to the records which further associates the image with the type of content, date, received, etc. Once this image has been fully indexed by FEMA, the Indexer clicks the archive button which then records all Meta Data in association with the image(s) and inserts the key Meta Data along with this image pointer location for future reference and information retrieval.

DMARTS allows FEMA authorized users to locate, access, store, retrieve, manage, and archive documents as well as create consistent, streamlined, supportable processes for FEMA employees and contractors. Consolidation of FEMA's document management functions into a single integrated content management system will increase the overall performance of the current system and streamline FEMA IT systems management by reducing the number of servers required, utilizing a single Storage Area Network (SAN) in their place; and replacing outdated servers with newer, faster state of the art equipment, improving

processing and retrieval speeds.

DMARTS may share information with outside agencies to assist in positively identifying registrants requesting Federal assistance. Information shared will be only that information necessary for approved components, with a need-to-know, to address each specific need as it arises, in accordance with the provisions of the Privacy Act, 5 USC Sec 552a.

DMARTS is a new system being developed for FEMA that will replace and supplement the systems identified below:

- Replace the ViewStar system
- Provide a repository for FEMA eGrants system
- Replace the current Tower TRIM system (this is currently under review)
- Provide integration with the National Emergency Management Information System (NEMIS)

Section 1.0 Information Collected and Maintained

Section 1 of this document defines the scope of information collected and the reason for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

Information will be collected from external clients such as individuals, states or agencies applying for Federal Emergency assistance. Data collected may include, but is not limited to:

- name
- NEMIS registration ID
- date-of-birth
- mailing address
- telephone number
- social security number
- email address
- zip code address
- facsimile number
- medical record number
- bank account number
- bank routing number
- education records
- health plan beneficiary number any other account numbers
- certificate/license number
- vehicle identifier including license plate, marriage record
- civil or criminal history information
- temporary address
- temporary phone number
- insurance policy number

- insurance settlement amount
- insurance coverage information
- estimates of damage to the home or personal property

In order for FEMA employees to access DMARTS, the system will rely on existing FEMA authentication and authorization systems, including the Integrated Access and Control System (ISAAC) and Active Directory; therefore, it will not contain biometric identifiers, photographic facial image, or any other unique identifying number or characteristic other than the user's logon ID.

1.2 From whom is information collected?

Information is collected from individuals, states, and/or agencies applying for disaster assistance benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, "registrants". It may be provided by the individual, state, other federal agencies or FEMA field operations. Data that is collected via this process is linked with registrant information stored in NEMIS.

1.3 Why is the information being collected?

DMARTS collects information from grant and assistant applicants to carry out FEMA's mission of assisting individuals who apply for disaster assistance benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

DMARTS collects SSN from individuals to assist with positively identifying registrants requesting Federal assistance, evaluate need, track payments and services, audit service delivery, identify fraud, and provide checks and balances for the Agency.

1.4 How the Information is Collected?

In accordance with the FEMA Privacy Act system of records, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), and as amended August 7, 2006, FEMA collects this personal information through applications in one of three ways. 1) Through applications in hard copy (paper) form when an individual fills out a paper application which may be mailed or faxed, or 2) by telephone interview, whereby an individual calls FEMA through a published disaster assistance phone number, and a teleregistrar reads all of the questions, and inputs the individual's answers directly into NEMIS, or 3) by electronic input via the Internet. NEMIS and other electronic information applications formerly used the ViewStar application to store files. These same files and information will now be stored in DMARTS.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The collection of information required for disaster assistance is based on the Robert T. Stafford. Disaster Relief and Emergency Assistance Act, 42 U.S.C. section 5121-5206 and the Homeland Security Act of 2002; Public Law Number 107-296(2002); 6 U.S.C 101 et.seq. The National Response Plan, Emergency Support Function #8, "Public Health and Medical Services Annex" also delineates responsibilities for providing health care and coordinating with the Department of Defense (DoD), Department of Veteran Affairs (VA)

and Department of Health and Human Services (HHS) in an emergency requiring implementation of the National Response Plan.

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

In order to carry out its mission to provide disaster assistance efficiently and effectively, FEMA must receive a significant amount of sensitive personally identifiable information. This allows FEMA to ensure it is providing assistance to the correct registrant for the correct reason in a timely fashion. Given the sensitivey of the information, FEMA has defined the system security under FISMA as confidentiality categorization of High. This designation requires FEMA to place additional security and access controls around the system. For example, DMARTS incorporates the Trusted Content Server option module for the base Enterprise Content Management (ECM) Documentum application to provide a basic level of security to the data while it is in the database. Additionally, FEMA has provided extra layers of security by encrypting data submitted via the web interface during transmission, placing hardware firewalls between the external user and the internal databases; ensuring faxed data is sent to an approved facility with proper physical controls and ensuring personnel handling the data have been properly cleared and trained. It is also a requirement of FEMA to manage access to data within a system maintaining PII data by developing Role based accesses. Each role (user account) is developed with a finite set of rules for accessing data.

Section 2.0 Uses of the System and the Information

The following sections delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Information from grant and assistance applicants is required to identify applicants, evaluate need, track payments and services, audit service delivery, identify fraud, eligibility including status in the U.S., and provide the checks and balances required by law.

In addition, information is collected to update an individual's temporary address, phone number and bank routing and account numbers for electronic funds transfers. The social security number may be used along with these other identifiers to positively identify the registrant, if the applicant supplies it. For most documents requested from applicants the SSN is not required.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "data mining")?

DMARTS itself does not analyze data, but manages data for analysis by other applications and by direct user interaction. The DMARTS application does not make determinations or conclusions based on the data it hosts. DMARTS does support the creation of business process workflows that facilitate the human review of information. These business workflow processes may append new or revised information to records maintained in NEMIS that will be accessible to government and state employees. This information will be used in accordance with the FEMA Privacy Act System of Records Notice, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), and as amended August 7, 2006 and published in the Federal Register July 6, 2006.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

DMARTS captures information provided by registrant, disaster field operations and Regions, as well as entered through other FEMA applications such as NEMIS. Information may be entered manually by operators, scanned from paper documents and from fax images or entered from Internet web sites and forms. Data validation is performed where possible using constrained value fields and by performing data lookups against previously-entered data such as registrant IDs or case numbers. Registrant ID and name are the most commonly used fields to associate a document with a registration. SSN is available less often, and is typically used when the registration ID and/or name can't be used to positively identify the registrant within NEMIS. DMARTS does not access commercial information aggregators to check the accuracy of entered information. The individual submitting the application must sign and verify that the information he or she has provided is true and correct to the best of the submitter's knowledge.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

To protect the large amount of PII collected and retained by DMARTS, access to the system is determined based on the job responsibilities performed by the worker (role based access). This provides for the "least privilege" rule. Meaning, persons have access to only the information required to complete their job responsibilities.

A system user (authorized and authenticated FEMA personnel) requires a FEMA network login ID and password. Once a user is granted access to the FEMA network their data access is controlled through Oracle database and application security mechanisms. Oracle grants data access in a hierarchical fashion. Meaning, access to DMARTS data is based upon a person's designated role. These roles are assigned specific "rights" or specific access (e.g., read only, modify, delete, etc.). The access granted is based upon a person's job responsibilities, assuring that the collected data is used only for its intended purpose. DMARTS retains a record of which documents an individual caseworker has looked at and indexed to provide an audit trail for sensitive information.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

DMARTS records related to registration for assistance, inspections reports, temporary housing assistance eligibility determinations, and eligibility decisions for disaster aid from other Federal and State agencies are covered by Records Schedule N1-311-86-1 4C10a and are destroyed after 6 years and 3 months.

DMARTS records related to State Files, independently kept by the State, which contain records of persons who request disaster aid, are covered by Records Schedules N1-311-86-1 4C7 and/or N1-311-86-1 4C10b and are destroyed three years after closeout.

All official records entered into DMARTS will be assigned a records schedule during the business work flow process based on FEMA Manual 5400.2, Section 5-11, Disaster Assistance Programs.

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

The DMARTS records retention schedules described in Section 3.1 are part of FEMA Manual 5400.2 dated February 29, 2000, and are approved by the Archivist of the United States. Coordination with the FEMA Records Management Office and FEMA Enterprise Architecture office to identify and properly configure the system for records retention based on the Tables and Rules associated with the data captured is planned.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Given the purpose of collected DMARTS data, the information must be retained for the indicated period. The preservation of official records is extremely important to allow future researchers and historians access to the history of FEMA, and to support the full auditing of public programs. The information collected by DMARTS includes administrative management, program, and information functions for financial assistance information involving public funds. Federal regulations and public law determine minimum retention periods for this data.

Section 4.0 Internal Sharing and Disclosure

This section is intended to define the scope of privacy information sharing within the DHS.

4.1 With which internal organizations is the information shared?

Information is shared internally with the following agencies:

- U.S. Immigration and Customs Enforcement
- FEMA Information Technology Services Division
- FEMA Office of the Chief Counsel
- FEMA Response Division
- Any DHS office that might provide guidance to the above-listed DHS offices.

Information shared will be only that information necessary for the DHS component, with a need-to-know, to address each specific need as it arises, in accordance with the provisions of the Privacy Act, 5 USC Sec 552a.

4.2 For each organization what information is shared and for what purpose?

DMARTS information such as: name, date-of-birth, mailing address, telephone number, social security number, email address, zip code address, facsimile number, medical record number, bank account number, education records, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, temporary address, temporary phone number, and bank routing number may be shared for the following purposes:

- U.S. Immigration and Customs Enforcement for the purpose of verifying an applicant's legal status to receive disaster assistance;

- FEMA Information Technology Division and contract personnel for maintaining and backing up all files that are created and stored in an electronic format;

- FEMA Office of the Chief Counsel for ensuring compliance with necessary laws and legal responsibilities;

- FEMA Office of Equal Rights for handling assistance disputes and inquiries, particularly if an applicant feels he or she has been discriminated against in disaster assistance decisions;

- FEMA Response Division, so that it may carry out its mission and perform necessary emergency assistance functions;

- DHS Components to provide guidance as specified in Section 4.1 above;

4.3 How is the information transmitted or disclosed?

Data is transferred electronically in a Federal Information Processing Standards Publication (FIPS) 140-2 approved encryption format from DMARTS to direct internal users or through connected end user applications such as NEMIS or EMMIE.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Given the requirements for sharing DMARTS data within a large enterprise wide network such as that maintained by DHS, there is a risk of data transmission eavesdropping. To mitigate this risk, all data transmission mechanisms will incorporate FIPS 140-2 approved encryption algorithms.

Section 5.0 External Sharing and Disclosure

This section defines the content, scope, and authority for information sharing external to DHS, including federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

As stated in the Disaster Recovery Assistance Files, DHS FEMA/REG-2, FEMA may collect and share privacy act information in the event of a Presidentially-declared disaster or emergency. Under this regulation FEMA shares information with federal agencies, state and local governments or other authorized entities for the purposes of reunifying families, locating missing children, voting, and with law enforcement entities in the event of circumstances involving an evacuation, sheltering, or mass relocation, for purposes of identifying and addressing public safety and security issues.

FEMA works closely with the Small Business Administration (SBA), and may share selected data with the SBA. Formalized agreements are in place with SBA for the information sharing to be limited to "official use" only for FEMA and SBA purposes. Any state government's access to data is limited to citizens of its own state. In both cases, access to the data is limited and controlled. Only authorized FEMA officials have access to the composite data source.

5.2 What information is shared and for what purpose?

Per the System or Records notice in section 2.2 above the categories of records that may be shared include:

(a) Records of registration for assistance that include individual applicants' names, addresses, telephone numbers, social security numbers, insurance coverage information, household size and composition, degree of damage incurred, income information, programs to which FEMA refers applicants for assistance, flood zones, location and height of high water level, and preliminary determinations of eligibility for disaster assistance.

(b) Inspection reports contain individuals' identifying information and results of surveys of damaged real and personal property and goods, which may include individuals' homes and personal items.

(c) Temporary housing assistance eligibility determinations. These refer to approval and disapproval of temporary housing assistance and include: general correspondence, complaints, appeals and resolutions, requests for disbursement of payments, inquiries from tenants and landlords, general administrative and fiscal information, payment schedules and forms, termination notices, information shared with the

temporary housing program staff from other agencies to prevent the duplication of benefits, leases, contracts, specifications for repair of disaster damaged residences, reasons for eviction or denial of aid, sales information after tenant purchase of housing units, and the status of disposition of applications for housing.

(d) Eligibility decisions for disaster aid from other Federal and State agencies (for example, the disaster loan program administered by the SBA, and disaster aid decisions of the state-administered Individual and Family Grants (IFG) and its successor program, Other Needs Assistance (ONA)) as they relate to determinations of individuals' eligibility for disaster assistance programs.

(e) State files, independently kept by the state, containing records of persons who request disaster aid, specifically for IFG and its successor program, ONA, and administrative files and reports required by FEMA. As to individuals, the state keeps the same type of information as described above under registration, inspection, and temporary housing assistance records. As to administrative files and reporting requirements, the state uses forms 76–32; PII data may be entered by processors if needed to validate/verify need, this is a free text field, , and 76–38; PII data requested includes the name of the applicant, their county/state and their signature.. This collection of information is essential to the effective monitoring and management of the IFG and the ONA Program by FEMA's Regional Office staff, who have the oversight responsibility of ensuring that states perform and adhere to FEMA regulations and policy guidance.

Any state or local government's access to data is limited to its own citizens. In both cases, access to the data is limited and controlled. Only authorized FEMA officials have access to the composite data source. Formalized agreements are in place with SBA for the information sharing to be limited to "official use" only for FEMA and SBA purposes.

5.3 How is the information transmitted or disclosed?

The required information is documented in the Memorandum of Understanding and an Interface Security Agreement between the Federal, State and Local government agencies and FEMA. The information is processed through documented systems interfaces specific to each agreement to ensure that each agency can access only the information necessary for their mission.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

FEMA has signed a Memorandum of Understanding and an Interface Security Agreement with SBA to ensure that it protects the privacy and the integrity of applicant's data. The SBA is granted limited access only to the information necessary to administer its program.

FEMA's Office of the Chief Financial Officer signs agreements with Treasury. The Chief Information Officer (CIO) of each agency signs the Memorandum of Understanding between FEMA and SBA.

All other information sharing fall under the routine uses described in the FEMA Privacy Act system of records notice, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), and as amended

August 7, 2006.

5.5 How is the shared information secured by the recipient?

Direct logon access to DMARTS is limited to FEMA employees using Government Furnished Equipment (GFE) configured and authorized by FEMA. Remote access is limited to FEMA VPN or iPass access. Security measures for those application systems are addressed in the individual system documentation (such as for NEMIS or the Integrated Security and Access Control System (ISAAC)). FEMA will review each information request and determine whether or not it meets the standards for sharing set out by the System of Records Notice. It does not provide electronic access to the information other than as specified in the System of Records Notices as stated in Section 5.2 above, and thus controls the information being provided.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Users are not required to take a training course prior to accessing information in DMARTS.

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

Given the external sharing of data collected and retained within DMARTS, there are privacy risks identified with the protection of the data by the external organizations. The specific risks identified are associated with inadequate security of information, or with inappropriate use of the information. These risks are mitigated by enforcing strict Memorandums of Understanding and Interface Security Agreements with these agencies, which detail their privacy protection requirements.

Section 6.0 Notice

Section 6 is 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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Notice is provided through all methods of collecting information. All paper forms include a Privacy Act notice. Where information is collected by Internet-connected systems such as EMMIE, those systems are required to post a privacy act statement online. Telephone interview operators provide privacy information to applicants.

To be eligible for assistance, all applicants must complete, sign and submit the DHS Declaration and Release form (90-69) which includes the notices that information provided may be subject to sharing within DHS and the Bureau of Immigration and Custom Enforcement. A copy of this form is available at http://r8.fema.net/Printable%20Forms/Shared%20Documents/Printable%20Forms/FF90-69.pdf.

In addition, the FEMA Privacy Act System of Records Notice, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), and as amended August 7, 2006, was published in the Federal Register on July 6, 2006
http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/E6-10640.htm.

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

DMARTS supports business process workflows that may not proceed to the next stage without the presence of required information. Failure of an applicant to sign the Declaration and Release form (90-69) will result in an ineligibility determination for the applicant. Applicants are informed that failure to submit the necessary information will result in the denial of assistance.

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

Individuals must consent to the use of privacy act data. Individuals authorize use of privacy act information by submitting a signed Declaration and Release form (90-69) in writing or online. This authorization is for all uses of the information as specified in the FEMA Privacy Act system of records, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), and as amended August 7, 2006.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Given the notice provided to individuals as defined above, no further privacy risks were identified.

Section 7.0 Individual Access, Redress and Correction

This section is 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 own information?

Individuals may gain information concerning their application's status by calling the FEMA Tele-registration Helpline at 1-800-621-FEMA (3362). Individuals may also gain access to their PII by accessing the FEMA internet application, Individual Assistance Center (IAC). Individuals create an account online to view their own application data, by creating an IAC account. The first time the individual creates their account, the SSN is used to validate their identity. A personal identification number (PIN) is then sent to the individual to complete the account creation process. The first time the individual accesses the application, the SSN is used in conjunction with the PIN to verify and authenticate the individual. The SSN is then no longer viewed within the application. The PIN and a password are then used for authentication to the application. Each individual is granted only limited access through the user id, password, and PIN to gain subsequent access, limited to viewing their own application data and/or viewing and updating their personal information record. Access to the data is granted in accordance with National Institute for Standards and Technology (NIST) Level 2 Assurance Level. Exposure of the data via the Internet is highly restricted and controlled in several layers to protect the data. No user accounts on the Internet are permitted direct access to the NEMIS database. The user's request for his specific record passes through three firewalls and the request is serviced by a trusted account behind the third firewall. The single record results are then passed back to the user, thus protecting the database. Each firewall serves to prevent unauthorized intruders from gaining access to systems behind that firewall. FEMA has implemented a series of these protection zones, which require successive penetration of each firewall to gain access to the subsequent. Applicants may request a copy of their file, which will allow them to receive copies of everything scanned into their record. DMARTS documents are also subject to FOIA requests. Requests should be sent to: FEMA Privacy Officer, DHS/FEMA, 500 C Street, SW., Washington, DC 20472.

7.2 What are the procedures for correcting erroneous information?

Applicants are asked to provide accurate information. Opportunities are provided in the written and online applications to perform a final review. The online forms provide review screens and edit buttons for correcting errors before submission. If an application or record update is submitted with erroneous information, the applicant may initiate corrective action through FEMA. Individuals may request a change to their own information and records by calling the FEMA Tele-registration Helpline at 1-800-621-FEMA (3362). When the information is processed, the individual's record is automatically updated to reflect the status of their specific application. An applicant may telephone to check on the status of and make updates to the personal information on their application. It is essential to maintain up-to-date information on the applicant to expedite application processing and render assistance quickly and equitably. NEMIS provides an internet access method enabling applicants to inquire about the status of their own applications, and to update their own personal data electronically.

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

Individuals are informed about the FEMA web site and tele-registration/Helpline through local radio, television, print media, and on the Internet. FEMA maintains an internet information site at: http://ia.fema.net which includes links for frequently-asked-questions, applicant's guides

(documentation), and an applicant inquiry link for registered applicants.

7.4 If no redress is provided, are alternatives available?

Redress is provided as described in Section 7.2 above, therefore no alternative redress mechanism is included in DMARTS. Alternative redress mechanisms may be provided through the Privacy Act and/or Freedom of Information Act (FOIA).

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Given the access and other procedural rights provided for in the Privacy Act of 1974, FEMA has provided access, correction and notification procedures related to the personally identifying information collected and retained in DMARTS.

Section 8.0 Technical Access and Security

This section describes technical safeguards and security measures used to protect privacy information.

8.1 Which user group(s) will have access to the system?

Access to DMARTS is limited to registered FEMA enterprise network users. This includes managers, system administrators, and contractors. Users from other DHS agencies, federal agencies, and state and local governments will not have direct access to DMARTS, but may access DMARTS content through approved FEMA applications such as NEMIS and EMMIE.

DMARTS is integrated with the existing FEMA enterprise authentication systems NEMIS Access Control System (NACS), Active Directory using Lightweight Directory Access Protocol (LDAP) and ISAAC. DMARTS relies on NACS, LDAP and ISSAC for user authentication and access control, as well as internal named user security. All users must exist in the FEMA enterprise authentication system before an account can be created or used in DMARTS.

DMARTS is based on the Commercial Off-the-Shelf application EMC Documentum®. Documentum® supplies all of the user and object security within DMARTS. Synchronization between Active Directory via LDAP and Documentum® is a standard Documentum® feature. The following user type authentication must occur to gain access to Documentum®:

Internal Users- Active Directory using LDAP. ISAAC is currently the provisioning starting point for Active Directory for those users who connect directly to the FEMA network to gain access to internal FEMA applications.

External Users - External users access DMARTS through existing FEMA applications via an externally-facing application (such as EMMIE) which authenticates the user through ISAAC and provides auditing of user actions, then requests services from the back-end FEMA infrastructure (e.g., Documentum®) through service accounts. The service accounts are subject to separation through security applied to the individual service account. State and local government's access to data is limited to its own citizens.

Direct Access – Users requiring direct access to the Documentum® interface are authenticated through Active Directory.

When the user logs on, Documentum® authenticates LDAP users via LDAP to the Active Directory server. Service accounts need not reside in Active Directory but are secured through an inline password with encryption. Authorization is controlled through group assignments.

The following types of logins have been identified:

- Login to Documentum® User Interface (Webtop) by end user
- Login through Documentum® Web Services with service account
- Login through Documentum® Web Services with principal user

8.2 Will contractors to DHS have access to the system?

DHS and FEMA contractors with authorized accounts in NACS / ISAAC will have access to DMARTS. DMARTS is being developed under contract by Information Manufacturing Corporation (IMC) under contract number HSFEHQ-04-A-0348. The development system is limited to IMC employee access. Test and Production systems are limited to users with FEMA authorized NACS / ISAAC accounts.

8.3 Does the system use "roles" to assign privileges to users of the system?

DMARTS utilizes ISAAC roles to assign groups, rights and privileges to authenticated users. These roles determine on an object bases which users have the rights to read, create, modify or delete information in DMARTS. ISAAC provides DMARTS with a system of role-based access controls and signature authorities. In ISAAC, access rights and signature authorities are assigned to specific positions in FEMA's day-to-day and emergency organizations. Each position within the organization has a set of roles, permissions, and authorities that have been approved by senior managers and all associated process accesses are directly related to the job responsibilities of a position. Personnel assignments to these job responsibilities may be fluid due to the nature of the FEMA mission, especially when operating under declared emergencies. DMARTS checks and synchronizes user roles and privileges with NACS / ISAAC on an ongoing basis.

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

DMARTS user access approval is accomplished through integration with NACS / ISAAC.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

DMARTS logs the time and date of each data record or information action (transaction), who completed it, the type of action, under what condition and/or function it occurred. DMARTS tracks all entries and modifications to DMARTS fields and records. All changes, including additions, modifications or deletions can be traced back to the originating user or connecting application, as well as the date and time the change occurred.

DMARTS does not internally maintain and is not authoritative for assignment of user roles. DMARTS queries ISAAC roles to assign groups, rights and privileges to ISAAC authenticated users. These roles determine on an object bases which users have the rights to read, create, modify or delete information in DMARTS. Integration exists between ISAAC and DMARTS / Documentum® for those applications dependent upon ISAAC authority. Users are authenticated in Documentum® through the Active Directory LDAP synchronization job. DMARTS logs all failed authorization attempts for auditing.

Auditing, security, and control for service accounts are enforced by the front-end application, e.g., NEMIS, EMMIE. These front-end applications access DMARTS using a service account, which does not identify the end-user, just the application. This service account is used to protect the documents within the repository. Auditing and security of the end user is controlled by the front-end application and not by DMARTS.

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

Audit logs for all DMARTS systems will be reviewed on a weekly basis by a DMARTS Information Systems Security Officer (ISSO). Any anomalies or security concerns encountered during the review of the audit logs will be documented and recorded in the DMARTS System Maintenance Log and reported appropriately. Audit logs will also be saved, cleared, and backed up every 90 days in order to maintain a historical record of the systems' audit logs for 7 years as required.

Additionally, DMARTS system events are monitored using the Nagios network monitoring tool. The software is configured to notify appropriate individuals of "critical" events via email so they can be investigated immediately. Detailed reports can also be generated from Nagios in order to accurately review and record all system events.

DMARTS itself logs the time and date of each data record or information action (transaction), who completed it, the type of action, under what condition and/or function it occurred. DMARTS tracks all entries and modifications to DMARTS fields and records. All changes, including additions, modifications or deletions can be reviewed and traced back to the originating user or connecting application, as well as the date and time the change occurred.

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

No specific privacy training is provided to users as part of DMARTS. All FEMA employees and contractors are required to complete FEMA Office of Cyber Security annual Security Awareness Training. All Contract employees are required to adhere to the Privacy Act / Confidentiality clauses as per the terms of their contracts with FEMA. Only authorized, trained users are granted access to the FEMA network and internal systems, including DMARTS, and only for authorized uses. If in individual is found to be misusing the information, appropriate disciplinary actions will be taken.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

DMARTS is designed to be compliant with FISMA requirements. Strong security controls have been instituted to ensure that the data repository is protected throughout all processes and functions. This includes extensive access controls, audit trails and encryption. This document has been prepared as part of the DHS Office of CyberSecurity Certification and Accreditation (C&A) Process. Authority to Operate letter was signed by the Authorizing Official on 10 October 2007. The current ATO will expire on 9 October 2010.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Given the privacy risks identified with the PII collected and retained by DMARTS, proper authentication and authorization of users is essential. DMARTS is integrated with the existing FEMA enterprise authentication systems NACS, LDAP and ISAAC. All users must exist in the FEMA enterprise authentication system before an account can be created or used in DMARTS. Authorization is strictly controlled by ISAAC roles.

Section 9.0 Technology

This section defines the analysis and selection process for technologies utilized by the DMARTS system.

9.1 Was the system built from the ground up or purchased and installed?

Competing technologies were assessed and compared for their ability to achieve system goals. For the primary system goals of document management and records management, several commercial-off-the-shelf packages as well as a proprietary package already in use at FEMA were considered. No single commercial package was available that filled all system requirements; however, all requirements can be met through integration of separate commercially available packages.

EMC Documentum® was selected as the best fit as the Electronic Content Management application for this project, based on its ability to perform the functions listed in the DMARTS requirements traceability matrix and it's listing on the FEMA Preferred Products/Standards list. EMC Captiva® was selected as the Document

Capture (scanning) solution based on available integration tools for Documentum®. Captaris RightFax® was selected as the FAX capture tool, based on the existing installed base of this software within FEMA.

Documentum® requires a relational database management system for the underlying data repository. Oracle Database Enterprise Edition was chosen for the ability to tightly integrate with the existing Oracle databases supporting NEMIS, ISAAC and EMMIE. Oracle Database Enterprise Edition is also listed as a FEMA Preferred Product/Standard.

Per recommendation by FEMA Enterprise Operations, RedHat Linux was selected as the preferred operating system wherever the application supported a Linux version. For those applications that are not supported under Linux, Microsoft (MS) Windows 2003 Server was selected. Both RedHat Linux and MS-Windows 2003 Server are included in the FEMA Preferred Products/Standards list.

Competing quotes and configurations of servers to support the DMARTS applications were evaluated. Through the competitive process a total system solution from Hewlett Packard Corporation (HP) was selected. This single-vendor solution of Severs, Storage and Backup simplifies integration, support and maintenance. A combination of HP DL380 servers, BL25p and BL45p server blades, HP EVA SAN storage and HP ESL SAN tape systems were selected. HP DL 380 Servers and SAN devices are listed as FEMA Preferred Products/Standards. HP BL series blades were under evaluation in the FEMATDL at the time of selection. The blade solution was selected due to the high number of servers required (over 50), reduced facilities support and its enhanced management features.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy and security were analyzed as part of the Certification and Accreditation process for DMARTS and following the DHS Certification and Accreditation Guidance for SBU Systems User's Manual. IMC performed requirements gathering and prepared a FIPS 199 Workbook, E-Authentication Workbook and Risk Assessment Document for DMARTS. As a result of this analysis process, DMARTS was determined to have a system protection level of High. IMC utilized the DHS Risk Management System to complete the DHS/NIST 800-37 questionnaire, creating a Requirements Traceability Matrix for the security controls.

Integration exists between ISAAC and DMARTS / Documentum® for those applications dependent upon ISAAC's authentication services. Users are authenticated in ISAAC and that authentication is conveyed to Documentum® using the user accounts established in the FEMA Secure Network Active Directory structure. The user is assigned localized groups in DMARTS if the definition of the users in the group matches the ISSAC roles held for the user. The assignment of users to groups is controlled by a synchronization process operating that runs on a recurring basis. Group definitions consist of criteria related to characteristics that 1) are not tagged with the object being secured (e.g., user must hold a certain position), or 2) match the characteristics carried with the object being secured (e.g., in the same region, for the same contractor). Documentum® recognizes reassignments within ISAAC in a reasonable time, so as not to dramatically impact the FEMA need to get user's security in place.

To control access to a set of documents (represented by a doc type) in Documentum®, a Documentum® group is created. In ISAAC, all positions within the organization that can potentially access the doc type are granted a role under the position that represents the Documentum® group. Since the user/group assignment must be near real-time, it is necessary to dynamically assign users to groups in Documentum®. With Documentum®, this typically occurs at login. Further, the Documentum® groups must be reflected in ISAAC, so the idea of a group definition must exist. This group definition associates a localized

Documentum® group to one or more ISAAC groups (defined as a home base + team + position + role + other discriminators). The definition must be made in terms of existence and non-existence of user authority within ISAAC using the discrete data elements present in ISAAC.

This dynamic capability allows FEMA to rapidly mobilize and engage personnel to effectively meet the needs of disasters and disaster victims in a timely and efficient manner.

9.3 What design choices were made to enhance privacy?

To enhance Privacy, including data confidentiality and integrity, IMC specified the optional Documentum® Trusted Content Server module. With this module, Documentum® is certified to meet Common Criteria Evaluation Assurance Level (EAL) 2. Using the Trusted Content Server, all repository data contained in DMARTS is encrypted and is not viewable in storage. This provides protection from viewing or manipulation by privileged system or network administrators. IMC also specified RedHat Linux 4 and Microsoft Window 2003 operating systems, which are certified to meet EAL4.

Conclusion

The FEMA DMARTS is designed to be the primary document and record repository for the FEMA Enterprise. It will provide FEMA with a formal, controlled environment for document and records management far superior to maintaining such records on diverse separate islands of servers and storage. Consolidating these documents, records and data objects improves privacy and security controls while providing authorized users enhanced abilities to locate, evaluate and process the information, thus improving productivity during disaster relief efforts. Records managers will also have enhanced capability to establish automated methods of designating official records, establishing and applying record retention actions, workflows and record archive activities. Implementation of DMARTS will improve FEMA's ability to provide control and audit capability of Privacy Act information.

Responsible Official

John A. Sharetts-Sullivan
FEMA Privacy Officer
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security