Privacy Impact Assessment for the

Standardized Tracking and Accounting Reporting System- Financial Management System (STARS-FMS)

United States Marshals Service

Contact Point
William E. Bordley
Associate General Counsel
Freedom of Information Act/Privacy Impact Assessment Officer, United States Marshals Service

Reviewing Official
Vance Hitch – Chief Information Officer
Department of Justice/Office of the Chief Information Officer
(202) 514-0507

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

Standardized Tracking Accounting & Reporting System—Financial Management System (STARS-FMS) is a major application owned by the United States Marshals Service (USMS) and is used to record and manage all financial information for USMS. This system supports budgeting and tracking of expenditures, and also financial reporting for all USMS appropriation and deposit funds.

STARS-FMS consists of two software application packages, supporting databases, and travel management services. The first application package, the Standardized Tracking Accounting and Reporting System (STARS) is used to record expenditures at USMS headquarters. The second application package, the Financial Management System (FMS), is used to record expenditures at the USMS district offices; the information recorded in FMS is ported into the STARS application at scheduled intervals. A payroll database containing information received from the National Finance Center is also a part of STARS-FMS; summarized payroll data is ported into the STARS application package at scheduled intervals. STARS-FMS users can access data from STARS-FMS via a secure network web browser.

Section 1.0
The System and the Information Collected and Stored within the System.

The following sections are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Personally identifiable information in STARS-FMS includes the following:

For USMS employees, the employee's name, employee number, social security number, home mailing address, and personal banking information including, savings or checking account numbers, bank routing numbers, name of the bank, and electronic fund transfer information. For temporary duty, STARS-FMS records include a portion of the employee's name, employee's social security number, locations of TDY and type of expense such as airfare or lodging. For relocations, STARS-FMS records include a portion of the employee's name, employee's social security number, moving expenses, travel expenses, and per diem.

For companies from which services are purchased by USMS, Tax Identification Numbers (TINs) are recorded in STARS-FMS. If a vendor does not have a TIN, as is sometimes the case for individuals providing services, the individual's social security number is used as the TIN.

For fact witnesses, who require reimbursement for travel costs, the social security numbers and mailing addresses of the individuals are used within STARS-FMS for payment and accounting purposes.

1.2 From whom is the information collected?

All personally identifiable information collected in STARS-FMS is provided directly by the individual and/or USMS personnel, or is systematically incorporated from payroll records, or the USMS contract travel agencies' records.

This information must be collected in order to ensure accurate financial recording and management of all financial information for USMS. The collection of the data supports budgeting and tracking of expenditures, and also financial reporting for all USMS appropriation and deposit funds. The use of data for banking or travel agencies is required in order for those organizations to provide services associated with USMS

financial expenditures, financial recording and management of USMS financial information.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following sections are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

STARS-FMS is used to record and manage all financial information for USMS. This system supports budgeting and tracking of expenditures and also financial reporting for all USMS appropriation and deposit funds. The personally identifiable information is collected to allow for accurate and timely payment of and tracking of individual expenditures associated with official USMS business.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

Upon acceptance of employment with the Federal government, an employee agrees to arrangements for processing payroll and the tracking of expenses (to include travel expenses) incurred on behalf of the employer. The user has also agreed to the terms of the Rules of Behavior for USMS Sensitive But Unclassified (SBU) Computer and Telecommunications Systems.

Fact witnesses give to the U.S. Attorney's Office information including their social security numbers or alien numbers and mailing addresses. This information is recorded in STARS-FMS so that payments can be made for travel of these individuals. The U.S. Attorney's Office handles the process of obtaining personal information from witnesses.

Vendors sign contracts which provide for payments to the vendors for services associated with USMS official business. The legal authorities for maintenance of the information in the system are 31 U.S.C. 3512 and 44 U.S.C. 3101.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Unauthorized access to and modification of data are privacy risks. The USMS has limited the collection of personally identifiable information to the minimum necessary to track expenditures.

In accordance with federal guidelines, STARS-FMS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained.

Some of the specific controls that address access to and modification of data include the following:

Personnel Security – A background check is completed on all personnel before they are granted access to the system

Physical and Environmental Protection – USMS controls all physical access points to facilities.

Access Controls – Supervisors complete account request forms specifying that accounts are needed to perform assigned duties before personnel are given access to the system. User permissions within the system are limited based on the roles supervisors have specified for each user.

Configuration Management – Security settings are configured to the most restrictive mode consistent with information system operational requirements.

Audit and Accountability – Audit logs record access to the system and modification of data.

Section 3.0
Uses of the System and the Information.

The following sections are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The personally identifiable information collected and stored in STARS-FMS is a critical component in the support of budgets, tracking of expenditures, and financial reporting for all USMS appropriation and deposit funds. The information is used to make and track USMS financial expenditures, to ensure the financial accountability of the individuals and vendors, to maintain accounts receivable and accounts payable records, and otherwise administer these and any other related financial and accounting responsibilities of the USMS.

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

STARS-FMS does not analyze data to assist users in identifying previously unknown areas of note, concern, or pattern.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

STARS-FMS and the associated data is subject to annual financial audits, configuration management/change management, certification and accreditation, and various manual reviews that ensure the accuracy of the system functionality and the associated data.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Information collected for this system will be maintained in accordance with National Archives and Records Administration (NARA) approved records retention schedules. Records are retained and disposed of in accordance with General Records Schedules 6 and 7.

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

There is a risk that someone performing budget-related tasks will view personally identifiable information.

In accordance with federal guidelines, STARS-FMS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained.

Some of the specific controls that address access to information include the following:

Personnel Security – A background check is completed on all personnel before they are granted access to the system

Awareness and Training – Users complete Computer Security Awareness Training before receiving access to the system

Access Controls – Supervisors complete account request forms specifying that accounts are needed to perform assigned duties before personnel are given access to the system. User permissions within the system are limited based on the roles supervisors have specified for each user.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following sections are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

The Department of Justice (DOJ) Justice Management Division (JMD) receives a file each month containing obligations, payments, collections, transfers and advances within Asset Forfeiture and Witness Security funds.

4.2 For each recipient component or office, what information is shared and for what purpose?

The information that is shared includes the following personally identifiable information: (1) when the vendor does not have a TIN, their SSN is used as the TIN, and (2) when an employee travels, their SSN is used as a vendor number. A portion of an employee's name is also included in accounting records regarding travel.

The information that is shared is used for the purposes of accounting for funds received and disbursed.

4.3 Information Transmittal and Disclosure

The information is transmitted over the USMS and DOJ networks. Depending on the situation, information may be hand-delivered, sent via fax, or conveyed telephonically to those persons who have a need to know the information for the performance of their duties.

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

There is a risk that information could be viewed or modified during transmission.

In accordance with federal guidelines, STARS-FMS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security

Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained. Privacy protections include strict access controls, passwords and role based access, tracking and audit features, and training for all employees and contractors.

Some of the specific controls that address protecting data during transmission include the following:

System and Communications Protection – The DOJ General Support System (GSS) Justice Unified Telecommunications Network (JUTNET) is used for transmission of the data.

Identification and Authentication – A password is used to authenticate to a DOJ system during the transmission process.

Section 5.0
External Sharing and Disclosure

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

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The information is shared with the following external (non-DOJ/non-USMS) recipients:

Travel agencies for authorized official travel

The Department of the Treasury for disbursement of funds

Other types of information sharing as set forth in the routine uses for the DOJ system of records notice entitled "Accounting Systems for the Department of Justice, DOJ-001," published in the Federal Register, [64 F.R. 29069 (May 28, 1999); 69 F.R. 31406 (June 3, 2004).

5.2 What information is shared and for what purpose?

Personally identifiable information that is shared includes the following:

For USMS employees, the employee's name, employee number, social security number, home mailing address, and personal banking information including, savings or checking account numbers, bank routing numbers, name of the bank, and electronic fund transfer information. For temporary duty, STARS-FMS records include a portion of the employee's name, employee's social security number, locations of TDY and type of expense such as airfare or lodging. For relocations, STARS-FMS records include a portion of the employee's name, employee's social security number, moving expenses, travel expenses, and per diem.

For companies from which services are purchased by USMS, Tax Identification Numbers (TINs) are recorded in STARS-FMS. If a vendor does not have a TIN, as is sometimes the case for individuals providing services, the individual's social security number is used as the TIN.

For fact witnesses, who require reimbursement for travel costs, the social security numbers and mailing addresses of the individuals are used within STARS-FMS for payment and accounting purposes.

Information is shared to pay, track, record, and reconcile USMS expenditures.

5.3 How is the information transmitted or disclosed?

A secure website is used by USMS and travel agency personnel to exchange data regarding travel.

A frame-relay circuit from a stand-alone computer and/or an encrypted channel from a networked computer on the USMS network are used to transmit data to the Department of the Treasury.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Technically there are no system interconnections and therefore no Interconnection Agreements. The data that is sent to the Department of the Treasury is placed on floppy disk and manually ported to a non-networked system, and then uploaded from the non-networked system via a frame-relay connection to Treasury. All agency components involved in the data sharing are required to abide by the Privacy Act of 1974—As Amended. Agencies are required to take appropriate action to protect personally identifiable information to ensure the means of transmission are secured by encryption or equivalent protections. Private entities that receive personally identifiable information from this system are required to secure this information and limit disclosure by a current Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) or a contract and by applicable federal laws.

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

All federal agencies are required to handle personally identifiable information in accordance with the Privacy Act and applicable System of Records Notices. In addition, federal agencies and their contractors are subject to information security requirements of the Federal Information Security Management Act (FISMA). DOJ is adding training regarding handling of personally identifiable information to their annual Computer Security Awareness Training, which is required annual training for DOJ and all of its components including USMS.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Internal Federal systems and all associated activities are subject to annual audits by the Office of the Inspector General. The USMS monitors the transmission of data to the external entities.

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

USMS will share information in this system only with those entities that have a need to know the information in order to perform their responsibilities. Additional sharing of this information will be in accordance with the applicable provisions of the Privacy Act and published system of records notices.

There is a risk that information could be viewed or modified during transmission.

In accordance with federal guidelines, STARS-FMS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained.

Some of the specific controls that address transmission of data include the following:

System and Communications Protection – An encrypted channel is used to transfer the data from USMS to a website at the travel agency.

Identification and Authentication – A password is used to authenticate to the website at the travel agency.

Section 6.0
Notice

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

6.1 Was any form of 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?

Yes. Notice has been given by publication of a DOJ agency-wide system of records notice in the Federal Register, [64 F.R. 29069 (May 28, 1999); 69 F.R. 31406 (June 3, 2004). In accordance with 5 U.S.C. 552a(e)(3) all forms, either paper or electronic, requesting personal information will provide a Privacy Act statement.

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

Monetary compensation for work and travel cannot be made unless the required information is provided. Individuals do not have the opportunity and/or right to decline to provide the information.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Individuals do not have an opportunity to consent to particular uses of the information. However, uses are limited as provided by the Privacy Act and the applicable System of Records Notice which has been published in the Federal Register.

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

Only the minimum amount of information needed for making payments and maintaining accounting records is recorded.

Individuals are provided a Privacy Act statement when information is collected setting forth the routine uses and purpose for collecting the information. However, providing the personal information is required.

Section 7.0
Individual Access and Redress

The following sections concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

In the event an individual USMS employee finds a discrepancy associated with his/her PII, the employee may contact the USMS IT Help Desk. The Help Desk is prepared to direct the individual to the appropriate change request forms and/or individual to make the necessary corrections. Individuals including vendors may also choose to request assistance from the USMS Office of Finance, the administrative officer within the office where they work, or the USMS Freedom of Information and Privacy Act Office. Individuals desiring access to or amendment of information maintained in this system may direct their request according to the Record Access Procedures set forth in the Department of Justice Privacy Act regulations, 28 C.F.R. 16.41 and 16.46, and the systems of records notice entitled, "Accounting Systems for the Department of Justice, DOJ-001," 64 FR 29069 (1999), stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

USMS Directives describing procedures related to the Privacy Act, finance, travel, and information technology services are published on the USMS intranet. Individuals desiring access to or amendment of information maintained in this system may direct their request according to the Record Access and amendment Procedures set

forth in the Department of Justice Privacy Act regulations, 28 C.F.R. 16.41 and 16.46, and the systems of records notice entitled, "Accounting Systems for the Department of Justice, DOJ-001," 64 FR 29069 (1999), stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Since individuals provide their personally identifiable information for input into the system, individuals are provided alternatives for correcting, updating and providing information through authorized individuals in the USMS offices that have access to the system.

Information that might need to be corrected/updated within STARS-FMS is of the following two types: (1) the identity (name and SSN) of employees who travel and are recorded in the vendor's table in STARS-FMS, and (2) addresses for fact witnesses.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

In the event an individual would like to contest information contained in STARS-FMS or actions taken as a result of USMS reliance on the information, they may contact the office responsible for the action, such as the Office of Finance. Individuals may also request access to or correction of their personally identifiable information pursuant to the Privacy Act.

Section 8.0
Technical Access and Security

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

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

User groups with access to the STARS-FMS System include USMS personnel and contract employees responsible for accounting for USMS financial expenditures and system maintenance, including information technology specialists, budget analysts, management analysts, and accounting specialists assigned to the Office of Finance, Management and Budget Division, Asset Forfeiture Office, and Information Technology Services. Administrative personnel performing budget functions within USMS offices also have access.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors have access to STARS-FMS. The USMS will initiate a review of all contracts to determine what role each contract has with respect to this PIA. Copies of related contracts will be provided at the conclusion of the review. All contractors are required to undergo suitability background investigations

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

Access to STARS-FMS system objects is limited based on the "role" of the user. For the STARS application, the supervisor identifies the role(s) of the user on the account request form, and the administrator assigns the role(s) to the user account. For the FMS application, the Office of Finance notifies the STARS-FMS program manager when a special role is required for an individual; documentation is completed and the role is assigned to the individual. The typical user of the FMS application works in support of a single USMS district; the supervisor for the user completes an account request form specifying which functions the user should be able to perform for that district, and the administrator enables those functions for the user account for the appropriate district's data only.

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

Procedures are in place for completing and processing STARS-FMS user request access forms. These procedures provide guidelines to ensure that all forms are processed in a consistent manner, users are assigned appropriate access in accordance with job functions, and that STARS/STARSWeb and FMS forms are properly authorized and retained. Additional procedures are in place to provide guidance on segregation of duties including which STARS functions are in violation of segregation of duties requirements.

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

User assignment of roles and rules are verified by validating STARS-FMS user accounts to ensure that only the privilege needed in STARS-FMS for job functions are granted and to ensure that current permissions are in compliance with Segregation of Duties requirements. On an annual basis, supervisors are required to review the list of users who have STARS-FMS access, to confirm that access is still needed, and to certify that the level of access is still required for the completion of the individuals' work responsibilities.

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

Security measures have been implemented in accordance with federal guidelines' categories of Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity.

Policies and procedures are in place for reviewing and monitoring audit logs to detect unusual or unauthorized events, and investigating security violations and taking appropriate actions. Logs show the date and time of events, what account initiated the event, from which system the event was initiated, and system performance parameters. Additionally, network activity logs are reviewed to detect unusual or unauthorized events that need to be addressed. Individual accountability is maintained because each account is assigned to a specific individual.

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

Computer Security Awareness Training is required of all users prior to granting them network access. This training includes general information on protecting sensitive and personal information. Annual ethics training is also provided to all users.

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

The data is secured in accordance with FISMA requirements. The certification and accreditation of STARS-FMS was completed on July 31, 2006.

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

Unauthorized access to and modification of data are privacy risks.

Data on the system is secured in accordance with applicable federal guidelines and standards. Security controls are in place to ensure confidentiality, availability, and integrity of personal data, including limiting access by function on a strict need to know

basis. In addition, administrative controls such as monitoring accounts, maintenance and review of audit trails, help to prevent or discover unauthorized access. STARS-FMS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained.

Some of the specific controls that address access to and modification of data include the following:

Access Controls – Supervisors complete account request forms specifying that accounts are needed to perform assigned duties before personnel are given access to the system. User permissions within the system are limited based on the roles supervisors have specified for each user.

Configuration Management – Security settings are configured to the most restrictive mode consistent with information system operational requirements.

Audit and Accountability – Audit logs record access to the system and modification of data.

Section 9.0
Technology

The following sections are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, Radio Frequency Identification Tags, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

N/A. Competing technologies were not evaluated to assess and compare their ability to effectively achieve system goals. STARS-FMS is not a truly new system. STARS-FMS is the combination of two USMS systems (the STARS system and the FMS system), which have been in place for several years. Updates and modifications have been made to apply the controls defined by current guidelines of the federal government.

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

N/A. STARS-FMS is not a truly new system. STARS-FMS is the combination of two systems (the STARS system and the FMS system), which have been in place for several years. Updates have been made to apply the controls defined by current guidelines of the federal government. Security and privacy controls have been designed to protect the confidentiality and integrity of the personal data in the system.

9.3 What design choices were made to enhance privacy?

Secure baselines have been implemented on all associated servers and controls have been established to ensure proper protection of privacy data. Only USMS employees and contractors, who are designated by their supervisors to perform roles within the accounting system and have been issued proper security badges and passwords, will have access to this system. USMS employees and assigned contractors receive training on the proper safeguarding of personally identifiable information. The system tracks access logs and maintains an electronic audit trail to protect against unauthorized access.

Conclusion

STARS-FMS is a major application owned by the USMS and is used to record and manage all financial information for USMS. This system supports budgeting and tracking of expenditures and also financial reporting for all USMS appropriation and deposit funds. STARS-FMS is a legacy system in the operations and maintenance phase of the system life-cycle. It is connected to the Marshals Network (MNET) General

Support System, which connects with the Department of Justice's network, which provides Internet connectivity.

The risks to the personally identifiable information stored and transmitted by STARS-FMS have been mitigated by USMS via security controls that were designed and implemented into the STARS-FMS application. These controls were reviewed and tested during the certification and accreditation of STARS-FMS, which was completed in July of 2006. This process ensures that risks to the PII stored and transmitted by the application have been reduced to a level deemed acceptable by the Chief Information Officer of USMS.

Responsible Officials

Diane Litman
Chief Information Officer
United States Marshals Service