



Department of Homeland Security Office of Inspector General

Audit of Application Controls for FEMA's Individual Assistance Payment Application





**Homeland
Security**

SEP 22 2009

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the results of the audit of the application controls for FEMA's Individual Assistance Payment process (IAP) within the National Emergency Management Information System (NEMIS) environment. We contracted the independent consulting firm, TWM Associates, Inc. (TWM) to conduct this audit. The contract required that TWM perform an application control review to ensure that adequate IT security controls are in place over the individual assistance payment application. It is based upon interviewing personnel responsible for implementing application internal controls, reviewing key documentation, and performing appropriate transaction tests.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

May 31, 2009

Jeannie A. Etzel
Chief Information Officer
Information Technology Division
Federal Emergency Management Agency
U.S. Department of Homeland Security
500 C Street, SW
Washington, DC 20472

Norman S. Dong
Chief Financial Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security
395 E Street SW, Mail Stop 3200
Washington, DC 20472

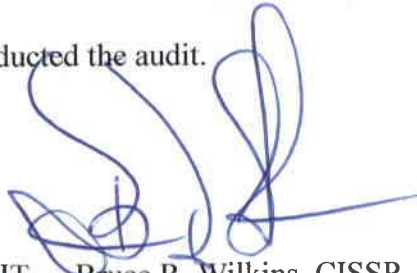
TWM Associates, Inc. (TWM) performed an audit of information technology security controls for the National Emergency Management Information System (NEMIS). The audit objective was to determine whether FEMA has implemented effective security controls over the individual assistance payment process within the NEMIS environment. This report presents the results of the audit and includes recommendations the agency can implement to enhance IT security controls over the NEMIS individual assistance payment process. We performed the audit as stipulated in Task Order TPDFIGBPA070015-0027.

We appreciate the opportunity to have conducted the audit.

Sincerely,



Lisa A. Johnson, CPA, CISA, CISM, CGEIT
Co-Owner



Bruce R. Wilkins, CISSP, CISA, CISM, CGEIT
Co-Owner

Table of Contents

Objectives, Scope, and Approach	2
Summary of Findings and Recommendations	3
Background	4
Results of Audit	5
Access Controls	5
Inspector Laptop Controls.....	6
Segregation of Duties.....	6
System and User Documentation.....	7
Approval and Payment Process	7
Recommendations.....	8
Access Controls	8
Inspector Laptop Controls.....	8
Segregation of Duties.....	8
System and User Documentation.....	9
Approval and Payment Process	9
Management’s Comments and OIG Analysis.....	9

Appendices

Appendix A: Overview of the IAP Completion Process in NEMIS	11
Appendix B: Management’s Response to the Report.....	12
Appendix C: Major Contributors to the Report.....	18
Appendix D: Report Distribution	19

Objectives, Scope, and Approach

We were engaged to perform an information technology application controls review of services related to federal disaster relief assistance applications and databases operated by the Federal Emergency Management Agency (FEMA). This audit supports the Office of Inspector General's (OIG's) requirement to determine if the Department of Homeland Security (DHS) has developed and implemented the proper level of internal controls to prevent, and detect fraud, waste and abuse for its national emergency management information technology systems, as required by Section 696 of the *Department of Homeland Security Appropriations Act, 2007* (PL 109-295). Section 696 of the *Department of Homeland Security Appropriations Act, 2007* states that all programs in FEMA that administer federal disaster relief assistance should develop and maintain proper internal management controls to prevent and detect fraud, waste, and abuse. This audit addresses controls in the National Emergency Management Information System (NEMIS), and specifically, the Individual Assistance Payment (IAP) process.

The objective of this audit was to determine whether FEMA has implemented effective security controls over the NEMIS IAP application. This audit does not address general IT controls nor controls addressed as part of the annual Fiscal Year (FY) financial statement audit or Federal Information Security Management Act (FISMA) audit. This audit required gaining an understanding of the NEMIS application, as well as reviewing and testing the application controls in place over the individual assistance payment application within the NEMIS environment.

Our independent audit focused on FEMA's implementation of internal controls, based on the requirements using the National Institute of Standards and Technology (NIST) special publication 800-53, companion guides for 800-53, Generally Accepted Government Auditing Standards (GAGAS), Generally Accepted Auditing Standards (GAAS), and *DHS Sensitive Systems Policy Directive 4300A and 4300B*, Version 6.1.1, October 2008. Additionally, we focused on supporting guidance from Section 696 of the DHS Appropriations Act of 2007, Government Accountability Office's (GAO's) Federal Financial Information Systems Controls Audit Manual (FISCAM), Office of Management and Budget (OMB) Circular A-123, Circular A-130, OMB Memorandum M-06-16 and best practice guidance. These requirements and guidance were utilized to determine the design and execution of the application controls audit and analysis of documentation provided by FEMA.

We conducted our audit between October 2008 and March 2009 in accordance with the authority of the *Inspector General Act of 1978*, as amended, and in accordance with GAGAS.

Summary of Findings and Recommendations

An application audit is a review of automated and manual controls within the business transaction process. We focused on the individual payments that flow through NEMIS. During the audit, FEMA was able to support and trace all transactions tested throughout the IAP application. However, we determined that FEMA needs to improve the controls over the IAP processing environment. We noted several weaknesses within the IAP environment such as physical and logical access controls over the inventory of laptop and tablet computers used by inspectors who gather IAP data. Specifically, these laptops contain weak password parameters, sensitive unencrypted Personally Identifiable Information (PII) data, and are stored in contractor controlled warehouses for which physical security review results have not been provided to ensure compliance with DHS requirements. In addition, there are no policies and procedures in place to ensure that the PII data is removed from these laptops in a timely manner. We also noted a lack of audit logging to track IAP transactions and the inspectors who are using Government Furnished Equipment (GFE) have not taken the annual FEMA or DHS refresher security awareness training.

We also identified a lack of required system and user documentation for the NEMIS IAP application. Documentation including system flow charts and narratives, user training manuals and user guides, were not available for our review. Documentation that was available and presented to the auditors did not provide sufficient detail of the IAP processing environment and was presented in draft format. A review of the IAP processing environment indicated that inspectors have the ability to input, validate and approve IAP claims, thus being able to circumvent segregation of duties in that they are the sole individuals who approve registrant information and input payment amount information. In addition, in emergency and disaster situations, IT controls can be turned off to expedite payment of IAP claims. There are no procedures in place to ensure that FEMA management goes back to formally review and approve these payments after the fact to ensure payments were properly made. We also found that payments requiring manual intervention are made without reviewing source documents.

We are recommending that the FEMA CIO and CFO:

- Improve logical and physical access controls to the NEMIS system, IAP process, and the laptop and tablet computers used to gather data for the IAP application,
- Strengthen segregation of duties over the input, approval, and payment of the IAP process, and
- Create and/or update NEMIS IAP system and user documentation.

Background

After Hurricane Katrina struck the Gulf Coast in August 2005, FEMA's mission to aid those in need called for an immediate response from the agency. NEMIS is a FEMA-wide system of hardware, software, telecommunications, services, and applications, providing an information technology base to FEMA and its partners for carrying out the emergency management mission. The purpose of this system is to support the FEMA mission critical applications and to do so with a general support system of uniform service oriented architectures. NEMIS is comprised of a combination of client server and web based applications and services. FEMA turned off many of the NEMIS system controls or checkpoints to speed the processing of payments for the individuals affected by Hurricane Katrina. Once FEMA turned these information technology controls off, the agency no longer had checks and balances in place over the IAP application. This action resulted in FEMA paying millions of dollars to ineligible individuals through the NEMIS system.

NEMIS is comprised of a series of independent and interdependent functional subsystems sharing the same platform, platform services, and mission. The public-face component of NEMIS supports hundreds of thousands of Federal, State, public, and local users. Upon an individual registering for assistance from a disaster, applicants' information including social security numbers, address information and other factors are communicated by FEMA to ChoicePoint, an independent company, to determine valid values. Registrant application information is shared with inspectors through the Auto Construction Estimation (ACE) system within NEMIS. The ACE system within NEMIS is utilized by two government contracting firms, Parsons Brinckerhoff (PB) and Partnership for Response and Recovery (PARR), to share information on individual assistance payment inspections. FEMA provides Government Furnished Equipment (GFE) in the form of ruggedized laptop computers and tablet computers to two contracting firms who provide and receive inspection information through the GFE to ACE. NEMIS assigns the inspections to be completed to inspectors, and then NEMIS shares the registrant application information with the inspector through the ACE system by interfacing with the inspectors' GFE tablet and laptop computers.

This audit addresses the IAP process that is handled through NEMIS. The recommendations should be considered by FEMA management to determine the appropriate manner for addressing them in the current and future NEMIS environment.

Results of Audit

Access Controls

- The inspector laptop computers containing PII and other sensitive data are not encrypted per OMB M-06-16 and *DHS 4300A*, Section 3.14.1, which requires that PII data removed from a DHS facility on laptops shall be encrypted.
- The individual assistance payment file containing PII data on the NEMIS system is in human readable format and is not encrypted.
- There is no evidence that IT controls are in place to ensure that duplicate payments are not paid from the IAP application. During our review of 25 case files, we determined that the duplication check function was scheduled to occur but found no evidence in the case logs that the function had been executed. Further, we could not validate that the subsequent duplication check had run prior to scheduled payments.
- Password configurations utilized on the contractor's GFE tablets and laptop computers are not required to be developed in accordance with *DHS 4300A*, Section 5.1.1.1 defining well-constructed passwords. For example, there is no requirement for passwords to be alphanumeric, eight characters long and using special characters.
- Contracted inspectors have not taken the DHS and/or FEMA annual security training or refresher training in accordance with *DHS 4300A*, Section 4.1.5 which indicates that all users (Federal employees as well as contractors) must perform security awareness training at least annually.
- Audit logging of systems events is not turned on for the NEMIS IAP system. Without audit trails, FEMA cannot ensure that all IAP data was properly input, processed and approved before payments were issued.
- Field-level security on the IAP web application is not tested and reviewed on a regular basis to ensure that unauthorized software code is not introduced into the application.
- PII data (for example, social security numbers and full names) are visible in the various IAP documents. Because the processing of IAP information involves a large amount of human intervention at various stages of the process, the risk exists that this unencrypted PII data can be accessed by unauthorized individuals.

- Some inspectors are employed by both contracting companies, PB and PARR. Our testing identified one inspector employed by the two different contracting companies who was assigned the same ID number for both companies within the NEMIS system. This system access structure caused confusion in the audit trail process when we attempted to track this individual's transactions back to their respective companies. As a result, individual accountability back to the respective contracting firm and inspector is not retained throughout the NEMIS IAP system.

Inspector Laptop Controls

- Inspector laptops contain unencrypted data and are maintained in contractor controlled warehouses. There is no evidence of physical security reviews being conducted to ensure DHS physical security requirements are adhered to for both GFE and GFE containing PII data. These laptops contain PII data gathered by inspectors for the IAP application. There is no requirement that the PII data on these laptops be removed in a timely manner. During our testing we noted one instance where an inspector laptop located in a contractor's warehouse contained PII data from the IAP application.
- FEMA does not ensure that contractor laptops contain the proper DHS security configuration and are included in the NEMIS certification and accreditation package in accordance with *DHS 4300A*, Section 3.3 that indicates contractor IT services and operations shall adhere to all applicable DHS information security policies.

Segregation of Duties

- Inspectors, who are government contractors, approve, validate, and input applicant information and payment specifics into the IAP application. The inspectors, by nature of the process, become the sole approving authority of inspection information, validate registrant identification, and perform data entry resulting in payment figures. As a result, inspectors could potentially misconstrue payment requests with valid information, and self-approve the IAP payment as there is no segregation of duties between the registrant, inspector, and person entering payment information. This could result in invalid or erroneous payments.

System and User Documentation

- The NEMIS System Security Plan (SSP) does not include application level documentation for the IAP application. The SSP needs to be updated to include IAP risk and controls matrix, process narratives, information flow diagrams; data architecture and program interdependency, system design materials, and user documentation such as NEMIS specific administrator and user guides and defined and assigned NEMIS application roles, including role of the application administrator.
- Of the system and user documentation provided, the documents were not granular enough to identify controls for the IAP processes. For example, adequate definitions of override codes used by FEMA employees to approve rejected system payments could not be provided. Without adequate system and user documentation, the risk exists that payments may be improperly authorized and paid to claimants.

Approval and Payment Process

- In the event of an emergency or disaster, the IAP application control routines can be altered, potentially allowing validation and approval of IAP claimant information to be temporarily turned off. FEMA has not established a process to go back after a disaster to ensure that the proper documentation and approvals are obtained for these transactions. In addition, because audit trails are not maintained for the IAP application, there is no way to ensure that all of these transactions have been captured.
- NEMIS contains fields to identify the type of information that each individual applicant provides during the inspection process and the date that this information was inspected. If an individual does not present this documentation during the inspection process, these supporting documents are not input into the system. If the applicant subsequently provides their information to FEMA, these items are entered into the IAP application; however, there is no process to review and verify the accuracy of this information. This process can lead to unauthorized or incorrect payments from NEMIS.

Recommendations:

Access Controls

We recommend that the FEMA CIO and CFO:

Recommendation #1: Implement proper password configuration settings for contractor laptop computers,

Recommendation #2: Encrypt sensitive and PII data and payment files,

Recommendation #3: Implement DHS required physical security controls at locations where there is sensitive and PII data in hardcopy format,

Recommendation #4: Require inspectors to take the annual security refresher training, and

Recommendation #5: Ensure application-level internal control routines are executed and the results of those routines logged in audit trails at a level of detail to ensure the expected internal control checks were executed.

Inspector Laptop Controls

We recommend that the FEMA CIO and CFO:

Recommendation #6: Encrypt sensitive NEMIS PII data on inspector GFE laptops and establish a process to ensure sensitive and NEMIS PII data is removed from the GFE laptops in a timely manner,

Recommendation #7: Require implementation of DHS required physical security controls for GFE laptops maintained at contractor facilities, and

Recommendation #8: Include the GFE inspector laptops in the NEMIS certification and accreditation process.

Segregation of Duties

We recommend that the FEMA CIO and CFO

Recommendation #9: Implement a quality assurance system to periodically review registrant source documents, registrant application information, and registrant payment inputs to ensure that inspectors cannot input, validate and approve registrant information without FEMA management oversight, and

Recommendation #10: Review and approve inspector gathered information to ensure cited items within NEMIS are supported.

System and User Documentation

We recommend that the FEMA CIO and CFO:

Recommendation #11: Review existing IAP application-level system and user documentation and ensure that it is current and reflects the IAP processing environment, and

Recommendation #12: Develop and implement the appropriate application-level system and user documentation.

Approval and Payment Process

We recommend that the FEMA CIO and CFO:

Recommendation #13: Review existing IAP application policies and procedures for validation and approval of IAP data during an emergency or disaster and update them to include proper approval of source documentation.

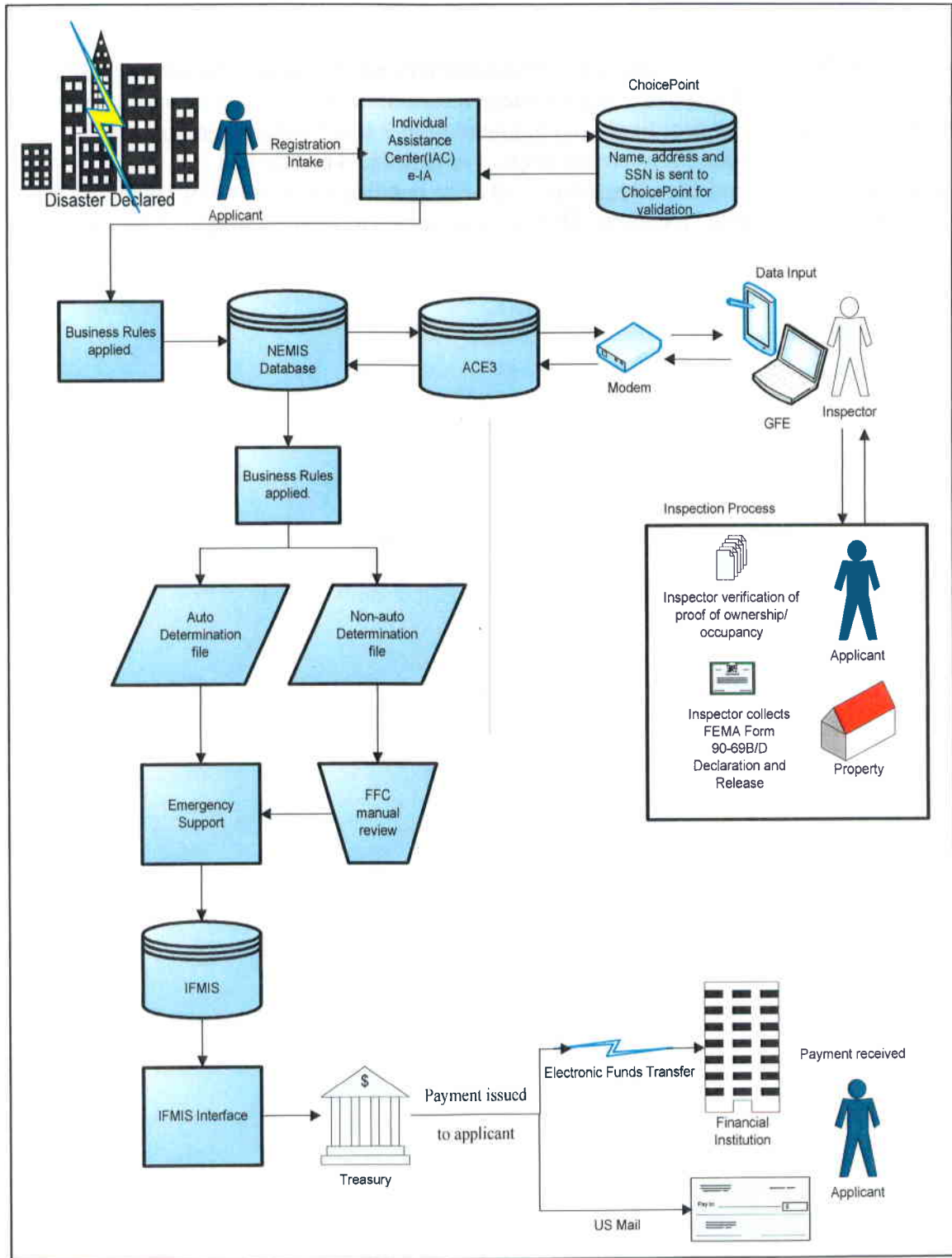
Management's Comments and OIG Analysis

We obtained written comments on a draft of this audit report from FEMA's Acting Director of Office Policy and Program Analysis. FEMA stated in its comments it needed more information to support the finding that there is no evidence that IT controls are in place to ensure that duplicate payments are not paid from the IAP application. In addition, FEMA stated it needed more information to support our finding that individual accountability back to the respective contracting firm and inspector is not retained throughout the NEMIS IAP system. To address these concerns, we have added information to our discussion of access controls.

In its comments, FEMA stated it did not concur with our finding that inspectors could misconstrue payment requests with valid information and self approve an IAP payment. We agree that inspectors do not have NEMIS system rights to authorize or approve payments. Still, we report that the inspector process lacks segregation of duties between the registrant, inspector, and person entering payment information. As a result, the current inspection method allows inspectors to approve, validate, and input applicant information and payment specifics into the system without independent verification from FEMA.

Generally, FEMA agreed with all of our recommendations except for recommendations numbers 2 and 5. FEMA stated it needed more information in order to respond to these two recommendations. Accordingly, recommendation 2 and 5 will remain unresolved pending further discussion between our respective offices. The other 11 recommendations are considered resolved and open pending verification of planned actions. We have included a copy of FEMA's comments in their entirety in Appendix B.

Appendix A Overview of the Individual Assistance Payment Completion Process in NEMIS



Appendix B Management's Response to the Report


U.S. Department of Homeland Security
Washington, DC 20472



FEMA

AUG 27 2009

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for IT Audits
Office of Inspector General

FROM: 
Robert A. Farmer
Acting Director
Office of Policy and Program Analysis

SUBJECT: Comments on OIG Draft Report, *Audit of Application Controls for FEMA's Individual Assistance Payment Application*

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG's) subject draft audit report. As the Federal Emergency Management Agency (FEMA) works toward refining its programs, the OIG's independent analysis of program performance greatly benefits our ability to continuously improve our activities.

FEMA has been diligently working to correct the issues identified in your audit. We submit the following comments concerning some of the audit's findings:

- *There is no evidence that IT controls are in place to ensure that duplicate payments are not paid from the IAP application.*

Response: FEMA requests that more information be provided to support this finding. Specifically, to what portion of the application is the OIG referring? There are business rules in place throughout the application to check and prevent duplicate payments.

- *PII data (for example, social security numbers and full names) are visible in the various IAP documents. Because the processing of IAP information involves a large amount of human intervention at various stages of the process, the risk exists that this unencrypted PII data can be accessed by unauthorized individuals.*

Response: FEMA must collect Personally Identifiable Information (PII) in order for the agency to carry out its responsibility to provide disaster assistance. Collection of this information is intended to benefit the applicant. Applicant banking information helps FEMA provide financial assistance efficiently via electronic transfer versus mail. Employees must enter this information so they will see it. In most cases, after registrations are processed without employee intervention (auto-determined) and only need approval. FEMA's auto-determination rate is very high in proportion to the number of cases worked manually.

www.fema.gov

Appendix B Management's Response to the Report

Page 2

FEMA restricts access to applicant PII data through its system of issuing user rights for the National Emergency Management Information System (NEMIS). Additionally, NEMIS keeps a record of each time an employee accesses an applicant's registration.

- *Some inspectors are employed by both contracting companies, PB and PARR. We noted that one of these contractors was assigned the same identifying ID number within the NEMIS system for both firms. As a result, individual accountability back to the respective contracting firm and inspector is not retained throughout the NEMIS IAP system.*

Response: FEMA requests that more information be provided to support this finding. NEMIS tracks inspectors using the INSPR_ID field. This is a unique number for every inspector. It is possible to have two or more inspectors with the same last name working for each contractor, but the INSPR_ID field would be different in the system.

- *Inspectors, who are government contractors, approve, validate, and input applicant information and payment specifics into the IAP application. The inspectors, by nature of the process, become the sole approving authority of inspection information, validate registrant identification, and perform data entry resulting in payment figures. As a result, inspectors could potentially misconstrue payment requests with valid information, and self-approve the IAP payment as there is no segregation of duties between the registrant, inspector, and person entering payment information. This could result in invalid or erroneous payments.*

Response: FEMA does not concur with this finding. The inspection process is designed to capture damages to an applicant's dwelling. Inspectors do not have NEMIS system rights to authorize or approve payments. FEMA must capture damage assessment data in order to determine applicant eligibility and authorize payments based on system business rules.

- *In the event of an emergency or disaster, the IAP application control routines can be altered, potentially allowing validation and approval of IAP claimant information to be temporarily turned off. FEMA has not established a process to go back after a disaster to ensure that the proper documentation and approvals are obtained for these transactions. In addition, because audit trails are not maintained for the IAP application, there is no way to ensure that all of these transactions have been captured.*

Response: The NEMIS system is hard-coded to require validation of Identity and Occupancy before any payments are sent to an applicant. During large events where normal system routines are altered in order to send payments to large groups of applicants, the program office still requires the verification of Identity and Occupancy for all payments. Should the payment be related to Home Repair, the program office would also keep the NEMIS control in place to verify Ownership. During large events, this verification is done through an external vendor that is used across the government for data validation. These controls are in place in all events. All payments, verifications, and events are recorded in the system of records, NEMIS.

Appendix B Management's Response to the Report

Page 3

- *NEMIS contains fields to identify the type of information that each individual applicant provides during the inspection process and the date that this information was inspected. If an individual does not present this documentation during the inspection process, these supporting documents are not input into the system. If the applicant subsequently provides their information to FEMA, these items are entered into the IAP application; however, there is no process to review and verify the accuracy of this information. This process can lead to unauthorized or incorrect payments from NEMIS.*

Response: Although we have put many fraud prevention controls in place and are consciously aware of the potential for fraud, we do offer emergency disaster assistance with the thought that most persons applying have a legitimate need for assistance and need it quickly. To do otherwise would put us at risk of being unable to help those who need help immediately.

Having said this, we believe there are additional prevention steps that we can put in place. GAO has recommended that we “establish random checks to assess the validity of supporting documentation submitted by applicants to verify identity and address.”

We have already begun discussions as to how we might do the random checks and have contacted the OIG to assist us with identifying some things that we can look for in fraudulent documentation, such as hotel bills with no logo. We will complete our discussions with the OIG and develop training to re-educate staff about the potential and types of fraudulent documents. We have made some organizational changes to include an internal Audit group that will report to the National Processing Service Center (NPSC) Operations Branch Chief. This new team will have the responsibility for conducting random checks, case reviews, working with the Government Accountability Office and the OIG, as well as others on lessons learned, review findings, and making recommendations for system changes. The manager should be in place no later than September 1, 2009.

With respect to the draft report's 13 recommendations, FEMA concurs with the recommendations with the exceptions noted below. While corrective action plans will be provided in our 90-day response, we provide the following information at the present time:

Recommendation 1: Implement proper password configuration settings for contractor laptop computers.

Response: FEMA concurs with this recommendation and is working to prepare a Plan of Action and Milestones (POA&M) to address the weakness. Remediation of this weakness is currently underway.

Recommendation 2: Encrypt sensitive and PII data and payment files.

Response: In order to respond to this recommendation, we need more information regarding how information would be encrypted and to which payment files this refers. FEMA must collect applicant PII in order for the agency to carry out its responsibility to provide disaster assistance. Collection of this information is intended to benefit the applicant. Applicant banking information

Appendix B Management's Response to the Report

Page 4

helps FEMA provide financial assistance efficiently via electronic transfer versus mail. Employees must enter this information so they will see it. Therefore, it would be very difficult to restrict employees from having access to applicant PII.

Recommendation 3: Implement DHS required physical security controls at locations where there is sensitive and PII data in hardcopy format.

Response: FEMA concurs with this recommendation and FEMA Management Directive 11042.1 requires such controls where sensitive and PII data are kept in FEMA facilities.

Recommendation 4: Require inspectors to take the annual security refresher training.

Response: The contractors do possess the training and we expect to have every inspector who deploys to disasters trained by October 1, 2009.

Recommendation 5: Ensure application-level internal control routines are executed and the results of those routines logged in audit trails at a level of detail to ensure the expected internal controls checks were executed.

Response: In order to respond to this recommendation, we need more information regarding the types of internal control to which this recommendation refers. The NEMIS Individual Assistance (IA) system records events for the cases in the events log. This log tracks all actions that take place for a registration. Additionally, for auto-determined eligibility decisions, a log is maintained of the specific NEMIS business rules that a case hits to receive an eligibility decision. Case processing and approvals are trackable using the events and business rule logs. FEMA's Office of the Chief Financial Officer (OCFO) does conduct internal audits of Individuals and Households (IHP) Payments as required by the Improper Payments Information Act.

Recommendation 6: Encrypt sensitive NEMIS PII data on inspector GFE laptops and establish a process to ensure sensitive and NEMIS PII data is removed from the GFE laptops in a timely manner.

Response: The OCIO's Information Technology (IT) Security Branch will ensure that the Disaster Assistance Directorate (DAD) project or program lead: 1) requires that sensitive NEMIS PII data on inspector GFE laptops is encrypted, and 2) establishes a process to ensure sensitive and NEMIS PII data is removed from the Government Furnished Equipment (GFE) laptops in a timely manner. The IT Security Branch will assist the DAD project or program lead in preparing POA&Ms, and will conduct quarterly advice and assistance oversight visits to ensure that the property IT security programmatic objectives are being met and maintained for the protection of PII data. In addition, on July 29, 2009, changes were made in the Automated Construction Estimator that stop the Social Security Number (SSN) from being sent to the inspection field unit, meaning that inspectors no longer have access to the applicant's SSN.

Recommendation 7: Require implementation of DHS required physical security controls for GFE laptops maintained at contractor facilities.

Appendix B

Management's Response to the Report

Page 5

Response: FEMA concurs with this recommendation.

Recommendation 8: Include the GFE inspector laptops in the NEMIS certification and accreditation process.

Response: FEMA concurs with this recommendation.

Recommendation 9: Implement a quality assurance system to periodically review registrant source documents, registrant application information, and registrant payment inputs to ensure that inspectors cannot input, validate and approve registrant information without FEMA management oversight.

Response: Inspectors do not have NEMIS system rights to authorize or approve payments. The inspectors capture damage assessment data in order to determine applicant eligibility. Payments are authorized based on system business rules. Additionally, quality control inspections are conducted to ensure adherence to FEMA policy and procedures.

FEMA concurs with the recommendation regarding implementing a system to periodically review registrant source information documents for authenticity.

Recommendation 10: Review and approve inspector gathered information to ensure cited items within NEMIS are supported.

Response: FEMA believes this recommendation is already standard practice. Line items are part of the Automated Construction Estimator software and the items are approved by FEMA and State officials. Inspectors cannot edit the line item. Additionally, Quality Control inspections are conducted to ensure that Inspector reports accurately reflect the damages to the applicant's property.

Recommendation 11: Review existing IAP application-level system and user documentation and ensure that it is current and reflects the IAP processing environment.

Response: The FEMA concurs with this finding. FEMA's IT Security Branch is currently working to separate the Individual Assistance Program (IAP) system as a Major Application and have its own Certification and Accreditation (C&A) under the NEMIS General Support System.

Recommendation 12: Develop and implement the appropriate application-level system and user documentation.

Response: The Office of the Chief Information Officer's IT Security Branch will ensure that DAD implements the appropriate application-level system and user documentation during the preparation of the application's C&A. Additionally, the IT Security Branch will assist DAD in preparing POA&Ms, and will conduct quarterly advice and assistance oversight visits to ensure that the proper IT security programmatic objectives are being met and maintained for application-level system and user documentation.

Appendix B

Management's Response to the Report

Page 6

Recommendation 13: Review existing IAP application policies and procedures for validation and approval of IAP data during an emergency or disaster and update them to include proper approval of source documentation.

Response: FEMA believes this recommendation is already standard practice. All of the IA policies and procedures are validated and approved prior to implementation during emergencies and during smaller disasters. NEMIS is hard-coded to require validation of Identity and Occupancy before any payments are sent to an applicant. During large events where normal system routines are altered in order to send payments to large groups of applicants, the program office still requires the verification of Identity and Occupancy for all payments. Should the payment be related to Home Repair, the program office would also keep the NEMIS control in place to verify Ownership. During large events, this verification is done through an external vendor that is used across the government for data validation. These controls are in place in all events. All payments, verifications, and events are recorded in the system of records, NEMIS.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on other issues as we both strive to improve FEMA.

Appendix C
Major Contributors to the Report

Information Systems Division

Sharon Huiswoud, Director
Sharell Matthews, Audit Manager
Steve Durst, Senior IT Auditor

TWM Associates, Inc.

Lisa Johnson, Government Contractor
Bruce Wilkins, Government Contractor
Harry Southerland, Government Contractor
James Ryan, Government Contractor

Appendix D Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operation
Chief of Staff for Policy
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Policy
Under Secretary, Management
Administrator, FEMA
DHS Chief Information Officer
DHS Chief Financial Officer
FEMA Chief Financial Officer
FEMA Chief Information Officer
Chief Information Officer, Audit Liaison
FEMA Audit Liaison
FEMA Acting Director, Office of Policy and Program Analysis

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.