Department of Homeland Security
Office of Inspector General

Improvement Needed in FEMA's Management of the National Flood Insurance Program's Information Technology Transition

OIG-10-76

March 2010

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 31, 2010

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 addresses challenges in the Federal Emergency Management Agency's National Flood Insurance Program's information technology transition. It is based on interviews with employees and officials, contractors, and a review of applicable documents.

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 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

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CONOPS	Concept of Operations
COTR	Contracting Officer's Technical Representative
CSC	Computer Sciences Corporation
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
IBM	International Business Machines
ISSO	Information System Security Officer
IT	Information Technology
NFIP	National Flood Insurance Program
OIG	Office of Inspector General
OST	Optimal Solutions and Technologies
PM	Project Manager
SOR	System of Record

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

At the request of the Federal Emergency Management Agency (FEMA), we reviewed the Mitigation Directorate's management and oversight of the National Flood Insurance Program's transition from its legacy information technology contractor, Computer Sciences Corporation (CSC), to a new contractor, Optimal Solutions and Technologies (OST). Although scheduled for 2008, the transition has yet to be completed.

The misplaced allegiances of key Directorate employees hampered the performance of both contractors. A former OST employee was chosen by FEMA to oversee OST's contract performance. In addition, approximately 14 former CSC employees worked in the Mitigation Directorate. The apparent inability of these employees to leave behind past alliances led to a divide within the Directorate and prevented an honest assessment of the status of NextGen and the transition.

The Mitigation Directorate attempted to develop an information technology system without the involvement of the Chief Information Officer, resulting in a system unable to meet FEMA's security and technical requirements. A lack of coordination with the Acquisition Management Division led to payment for an unproven system.

Mitigation Directorate officials gave orders to the contractors without the involvement of contracting personnel. This undermined the contracting officer's ability to enforce the terms of the written agreements between the contractors and FEMA.

The current acting assistant administrator for the Mitigation Directorate admitted knowing little about information technology, the status of the transition or agency security requirements. For too long he relied on subordinates rather than seek assistance from the Chief Information Officer and the Acquisition Management Division.

We made four recommendations to improve FEMA's oversight of information technology systems. FEMA agreed in part with one recommendation and in principle with the remaining three.

Background

The U.S. Congress established the National Flood Insurance Program (NFIP) in 1968 in response to severe flooding following a series of hurricanes in 1963, 1964, and 1965.[1] The key policy objectives of the NFIP were to: (1) reduce the Nation's flood risk through floodplain management; (2) improve flood hazard data and risk assessment by mapping the Nation's floodplains; and (3) make affordable flood insurance widely available in communities that adopt and enforce measures that make future construction safer from flooding. FEMA's Mitigation Directorate manages the NFIP and a range of mitigation programs designed to reduce future losses associated with disasters.

The private sector participates actively in the NFIP by writing and servicing flood insurance policies, developing and maintaining the information technology (IT) infrastructure, identifying and mapping special flood hazard areas, and providing technical and consultative support to states and communities. FEMA has agreements with more than 80 insurance companies to sell and service flood insurance through the "Write Your Own" program. As of August 2009, there were 20,000 participating communities and more than 5.5 million active policies in the United States.

The NFIP policy and insurance data generated nationally by the Write Your Own program insurance companies is collected and reconciled by FEMA's Bureau and Statistical Agent. Beginning in 1983, the administration of the Bureau and Statistical Agent, along with other NFIP services such as IT, training, customer service, and marketing, had been provided by one contracting entity Computer Sciences Corporation (CSC). CSC is a large publicly traded company with an extensive history of supporting federal contracts.

From 1999   2002, FEMA, with assistance from Booz Allen Hamilton, developed a blueprint for modernizing the NFIP's future operations (Concept of Operations (CONOPS)). The CONOPS and ideas generated at meetings among government and industry professionals determined the requirements for the NFIP's new IT system, known as NextGen. Optimal Solutions and Technologies (OST) was awarded a contract in 2003 to develop NextGen, a government owned system to be utilized by the NFIP, Write Your Own program insurance companies, and federal contractors.

[1] The National Flood Insurance Act of 1968 (P.L. 90-448, Title XIII), codified in 42 U.S.C. 4001 *et seq*.

During the life of its contract, OST was to develop multiple stakeholder program functions for NextGen. This new system was designed to replace the legacy system of record (SOR)[2] operated by CSC, which was scheduled to be retired in October 2008. The new system would provide stakeholders with a web-based interface through which data could be easily entered and queried. During development of NextGen, CSC continued to administer and support the multiple NFIP activities.

NFIP IT Services Timeline

(1968   2007)

1968

- Congress establishes the National Flood Insurance Program (NFIP)

1983

- FEMA contracts with CSC to provide multiple NFIP services

1999 – 2003

- FEMA reengineers the NFIP's concept of operations plan
- Based on the concept of operations plan, FEMA contracts with OST to develop new IT system called NextGen

2006 – 2007

- CSC provides OST with data to assist OST with the development of NextGen
- FEMA hires former OST NextGen Project Manager (PM) as the Information System Security Officer for both CSC and OST
- FEMA accepts and pays $40 million for NextGen conception and development
- Former OST NextGen PM becomes COTR for IT services contract with OST
- FEMA contracts with Apptis, an IT firm, to conduct IT evaluation of NextGen
- FEMA announces plans to break up CSC legacy NFIP contract into multiple components when current contract expires

Source: FEMA, CSC, and OST

In 2007, the Bureau and Statistical Agent contract came up for renewal. In an effort to increase the use of small businesses in DHS, FEMA re-competed the previously large Bureau and Statistical Agent contract portfolio (CSC was the sole contractor) as multiple separate contracts, including the Bureau and Statistical Agent, information technology services, training, and call center services. The latter three were set aside for small businesses, and OST was awarded the IT services contract. OST is a small,

[2] A system of record is an information storage system which is the authoritative data source for a given piece of information. In the case of the NFIP, output data is collected from multiple insurance companies and other stakeholders, and then reprocessed and re-presented in reports for FEMA, Congress, and other NFIP stakeholders.

minority owned IT firm, founded in 1999. As a result of this award, OST assumed responsibility for transitioning the SOR from the legacy system run by CSC to NextGen, the new IT system that had been developed by OST under its 2003 contract. During an agreed-upon period, CSC was to work with NFIP staff and OST personnel to transition historic NFIP data from the CSC IT systems to NextGen.

Results of Review

Misplaced Allegiance of FEMA Employees

The misplaced allegiance of many FEMA employees in the Mitigation Directorate hampered the performance of both contractors involved in the transition to a new IT system.

In 2006, the NFIP Program Office (Program Office) hired an OST employee who had worked for several years on the development of NextGen. In 2007, this employee served as a non-voting, IT advisor to the panel selecting the contractor to provide program management and insurance services in support of the NFIP. This person's former employer, OST, was one of the bidders and was awarded the contract.

After the expiration of one year of employment at FEMA,[3] the former OST employee was selected by the Program Office to be the contracting officer's technical representative (COTR) for the OST contract (hereafter, the former OST employee will be referred to as the OST COTR). As the OST COTR, he was responsible for ensuring adherence to contract terms, timely and acceptable deliverables, and payment upon satisfactory completion of services. COTRs report to contracting officers and serve as their eyes and ears. A FEMA COTR's sole allegiance must be to FEMA and he must be willing to advise the contracting officer when problems arise with a contractor's services. However, the line between the OST COTR's allegiance to FEMA and OST became blurred and may have delayed the Program Office's realization that NextGen was unable to become the SOR as scheduled. For example, the OST COTR misrepresented to staff the results of an independent IT analysis of NextGen in March 2008, portraying the findings more favorably than actually

[3] 5 CFR 2635.502 provides standards of ethical conduct for federal employees and prohibits their participation in certain activities involving past employers until one year has elapsed since that employment.

reported. As recently as spring 2009, the OST COTR asserted that the analysis indicated the NextGen transition could occur with minimal risk and demonstrated that OST had successfully delivered the required systems. However, the 2008 report on NextGen concluded:

- The requirement (business logic) documentation is not complete,
- The system is not fully tested, and
- Full Unit Testing should be conducted to find any additional latent defects prior to implementation.

Additionally, he assured Program Office personnel that NextGen was ready to become the SOR for the NFIP, knowing that the system lacked an "Authority to Operate," an approval from FEMA's IT Security Office that is required before an IT system becomes operational.[4] The OST COTR was aware of this security requirement. Lastly, the OST COTR failed to advise the contracting officer when contract milestones were not met, a possible breach by OST of contract terms. OST was unable to transition NextGen as the SOR for the NFIP as scheduled in May and October 2008, nor in 2009, but the OST COTR did not alert the contracting officer to these missed milestones, and the first cure notice to OST was not issued until July 2009.

The problem of misplaced allegiance extended beyond the issues associated with the OST COTR. Approximately 14 former CSC employees also worked at different levels of management in the Program Office. According to the FEMA employees we interviewed, these former CSC employees and other FEMA officials referred to CSC as "we" at internal meetings; told an acquisition official that OST had to "prove itself;" shared internal communications with CSC employees; and when disputes arose between FEMA and CSC, took the side of CSC.

Without exception, interviewees voiced concern that the Program Office had split into two camps, those favoring CSC and those favoring OST. The risk insurance portion of the NFIP is a niche program which involves a small group of government staff, contractor employees, and public stakeholders. Contractor and stakeholder employees are often hired by FEMA, and some FEMA employees leave to work in NFIP-related activities in the private sector. FEMA staff treat this "revolving door" with little concern for the divisive atmosphere it generates. Recently, and possibly as

[4] DHS Sensitive Systems Policy Directive 4300A, Version 7.0, July 31, 2009.

a result of this review, FEMA removed the former OST employee from his COTR responsibilities.

Conclusion

The apparent inability of some FEMA employees to leave behind past alliances with private industry, and favoritism for the legacy contractor that grew over several decades, may have impeded the timely completion of contract services. Because NextGen did not become the SOR as scheduled, FEMA needed CSC to continue to operate the legacy NFIP IT system for an additional year, at a cost of more than $7.2 million. Additionally, FEMA engaged International Business Machines (IBM) to analyze NextGen's readiness; IBM's initial work cost FEMA $388,000. On November 18, 2009, FEMA terminated the OST contract for convenience. This action will save the government a sum indeterminable at this time, and will decrease the cost of the delay discussed above.

Recommendation:

We recommend that the Administrator, Federal Emergency Management Agency:

Recommendation #1: Require that all employees involved in the procurement process receive annual procurement-specific ethics training and file financial disclosure forms. Employees involved in the procurement process include contracting officer's technical representatives and members of, and advisors to, source selection boards. Although ethics training is not required to be conducted in person, we believe the training would be most effectively delivered in person by the FEMA Ethics Office, to enable active participation in a class specifically tailored to the Program Office's needs.

Management Comments and OIG Analysis

The Office of Policy and Program Analysis concurred in principle with this recommendation. It states that all FEMA employees receive ethics training and those regularly working with contractors are required to take additional training geared toward procurement and other related ethics issues that arise when federal employees and contractors interact in the federal workplace. The Office further states that requiring all employees involved in the procurement process to file financial disclosure forms would be overly burdensome to reviewing officials and that the current requirement covering all employees who make substantive decisions in the procurement context is adequate. We disagree with this limitation, but agree that the contracting officer's technical representatives and task monitors not currently serving in those capacities can be excluded from the requirement until assigned to a contract.

Better Coordination Needed Among the Mitigation Directorate, Office of the Chief Information Officer and the Acquisition Management Division

For many years, FEMA program offices had their own IT staff and budgets, and developed IT systems without input or guidance from Acquisition Management or the Office of the Chief Information Officer. The development of the NextGen system is an example of an IT system developed by a program office outside the purview of the Chief Information Officer.[5] The Program Office's failure to work with the Chief Information Officer and Acquisition Management staff as strategic partners in the acquisition and development of NextGen resulted in the waste of approximately $7.5 million and delayed the implementation of a system intended to provide up-to-date data needed by the NFIP's stakeholders.

The Federal Information Security Management Act (FISMA) requires federal agencies to demonstrate to the Office of Management and Budget that its IT systems are compliant with IT security standards and requirements. Before FEMA allows an IT system to become an SOR, collecting, maintaining, and reporting personal data, the system must be tested and be shown to include controls that will protect private and sensitive information. A system that is certified and approved is given an Authority to Operate by the FEMA Office of the Chief Information Officer.

In 2007, the CSC legacy system was found to have deficiencies, but was accredited and allowed to operate. The IT Security Office had few staff and many systems to test, and put its efforts elsewhere. In preparation for the next FISMA report, CSC's

[5] DHS Management Directive 0007.1, Information Technology Integration and Management, issued March 15, 2007, requires the Chief Information Officer, in conjunction with the Chief Procurement Officer, to review and approve IT acquisitions in excess of $2.5 million. Office of Management and Budget Circular A-11, Part 7, Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets, establishes policy for planning, acquisition and management of major information technology investments. These policies, if followed, should eliminate problems created by FEMA Program Offices attempting to develop IT systems on their own.

legacy system was reviewed and again found inadequate. Documentation supporting processes did not stand up to testing. An IT Security official said she believes that the legacy system did not include the necessary controls because Program Office personnel did not have the IT expertise necessary to ensure required controls in the system, and no assistance from FEMA's IT Security Office was ever sought. This official claimed that for years there was friction between FEMA's Chief Information Officer and the Mitigation Directorate.

The development of NextGen began in the Program Office in 2003, and the FEMA Chief Information Security Officer said that she did not learn of the existence of NextGen until the Program Office sought an Authority to Operate in 2008. Believing initially that NextGen was going to become the SOR for the NFIP in late 2008, the IT Security Office was prepared to allow CSC's legacy system's Authority to Operate to expire in October of that year. However, it became apparent that NextGen was not ready to become the SOR, and NFIP officials asked that the CSC legacy system be permitted to operate instead. NextGen was then removed from the 2008 list of operating IT systems and placed in the development queue.

Program Office Management of an IT System

At the request of the OST COTR, the IT Security Office began the certification and approval process for NextGen in early 2009. The process consists of a review of system documentation and testing. IT Security Office staff who reviewed the documentation noted that some of the data fields only contained the words "to be determined," evidence that NextGen was not ready to be the SOR. The Program Office and Acquisition Management, working without assistance from the Office of the Chief Information Officer, paid $40 million to conceptualize and develop NextGen without testing the system to see if it performed according to the contract requirements.

Additionally, the NFIP IT Consensus document supporting the award to OST indicates the evaluation team considered the development of NextGen a "strength," even though the document provides no evidence that NextGen was tested and found to provide accurate, reliable data. Further, the Consensus document notes that OST's proposal indicates an understanding of the importance of pilot testing, yet the evaluation team failed to request evidence that any testing had been conducted to date. The fact that NextGen remained unproven through 2009 raised concerns regarding the thoroughness of acquisition planning, monitoring of contracts, and the contract award process at FEMA.

In addition to his official duties on the OST contract, the OST COTR simultaneously served as a COTR and as an Information System Security Officer (ISSO) for both the CSC legacy and NextGen systems. Section 2.1.8.e of DHS Directive 4300A, Sensitive Systems Policy Directive, states that ISSO duties shall not be assigned as collateral duties unless approved by the Component Chief Information Security Officer. No such approval was granted.

NFIP IT Services Transition Timeline

(2008 2009)

2008

May:	NextGen originally scheduled to go live as SOR
Oct.:	NextGen again scheduled to go live as SOR
Nov.:	New Acting Federal Insurance Administrator of the Mitigation Directorate appointed
Nov.:	NFIP managers commit to resolving all data integrity issues by 12/2008

2009

Jan.:	NextGen still not ready
Apr.:	Contracting Officer directs termination of the CSC or OST contract
May:	Mitigation Directorate announces plans to terminate the OST contract
Jun.:	FEMA Administrator overturns decision to terminate the OST contract
Jul.:	DHS-OIG requested to evaluate NFIP IT services transition
Aug.:	IBM requested to conduct technical evaluation of NextGen
Oct.:	OST COTR relieved of his duties
Nov.:	OST IT services contract terminated

Source: FEMA, CSC, and OST

The NFIP IT legacy system was to be replaced by the new NextGen system first in May 2008, then October 2008, and then in 2009. As of the writing of this report, the legacy system remains the SOR. Because the ability of NextGen to operate as required was uncertain, FEMA contracted with IBM to conduct an independent technical assessment of NextGen. To date, an assessment of the system's documented requirements has cost FEMA more than $388,000. The initial finding from IBM is that OST did not document the requirements, and the requirements provided by the Program Office to OST were poorly defined and need to be rewritten before further development of the IT system.

Conclusion

Because the Program Office did not work jointly with Acquisition Management and the Office of the Chief Information Officer during NextGen's development, FEMA was forced to continue the CSC contract for another year. Additionally, FEMA spent $40 million for an IT system without determining if the system operated as required and paid more than $388,000 for the first step of a full assessment of the system.

Recommendation:

We recommend that the Administrator, Federal Emergency Management Agency:

Recommendation #2: Ensure that the Acquisition Management Division and the Office of the Chief Information Officer work as strategic partners with program offices in developing information technology acquisition plans, and require the Office of the Chief Information Officer to test and approve all new information technology systems prior to acceptance by the contracting officer and final payment. This includes all future development and maintenance of NextGen, and other National Flood Insurance Program information technology systems.

Management Comments and OIG Analysis

FEMA's response is only partly responsive. The recommendation requires all FEMA program offices to work with the Office of the Chief Information Officer and the Acquisition Management Division as strategic partners in developing information technology systems prior to acceptance by the contracting officer. Additionally, the recommendation includes any further development of NextGen. FEMA's response only refers to further development of NextGen. Our recommendation was meant to cover *all* new FEMA information technology systems.

Contract Management Interference

The NFIP Program Office within FEMA's Mitigation Directorate has undermined the authority of Acquisition Management, the contracting officer's handling of the NFIP-related contracts, and his appointed technical representatives. As a result, the contracting officer was unable to enforce the terms of the OST contract in FEMA's best interests.

During the latter portion of 2008, a new contracting officer was appointed for the NFIP's IT services contract (hereafter, the NFIP contracting officer will be referred to as the Contracting Officer). As such, he is the person within Acquisition Management having oversight authority and managerial responsibility for FEMA's three NFIP services contractors, CSC, OST, and iServices.[6] To assist the Contracting Officer and provide technical insights about the NFIP, the Mitigation Directorate selected two federal employees as COTRs, one for the legacy CSC and iServices contracts, and one for the OST contract.

As noted earlier, the Mitigation Directorate has fractured into two camps, those supporting the legacy contractor, CSC, and those that support the developers of NextGen, OST. This organizational division made managing the contracts difficult because the Contracting Officer could not trust his COTRs to give him objective insights into the companies' abilities to perform under the contracts. Additionally, the Program Office as a whole undermined the Contracting Officer's ability to act in FEMA's best interests when enforcing the terms of the contracts.

For example, according to the Contracting Officer and others, Program Office staff participated in secretive meetings with CSC and OST, outside the presence of the Contracting Officer or his technical representatives. The acting assistant administrator and his managers were giving orders to CSC and OST which could be taken as oral modifications to the contract terms when only the Contracting Officer had the authority to modify the contracts. Even after the Contracting Officer instructed the Program Office's leadership to stop this practice, the meetings continued.

These unauthorized meetings undermined the authority of the Contracting Officer and prevented him from determining if either CSC or OST was in breach of their respective contracts and from

[6] iServices is a team of contractors led by OST as the prime contractor currently providing certain NFIP services.

issuing appropriate cure notices. The Contracting Officer also received conflicting reports from Program Office staff as to who was to blame for OST's inability to take over responsibility for the NFIP IT system as scheduled. Many weeks went by while staff argued over whether CSC was undermining OST by refusing to provide data OST needed for the NFIP IT transition or whether the data was being provided as required, but the NextGen system was unable to accept it due to flaws in the NextGen system.

Conclusion

The Program Office's unauthorized meetings with the contractors undermined the Contracting Officer's ability to enforce the terms of the contracts. Additionally, the Program Office's staff did not alert the Contracting Officer to possible lapses in contract performance. These actions contributed to the Contracting Officer terminating the OST contract for convenience of the government, rather than for default, resulting in additional expense to FEMA.

Recommendation:

We recommend that the Administrator, Federal Emergency Management Agency:

Recommendation #3: Ensure that Mitigation Directorate staff receive annual training on the roles and responsibilities of the contracting officer, and the contracting officer's technical representative. This training shall include instruction on appropriate interaction with contractor staff. For the same reasons set forth in Recommendation #1, we believe this training would be most effectively delivered in person by FEMA's subject matter experts from the Ethics Office, the Acquisition Management Division, and other offices, as needed.

Management Comments and OIG Analysis

FEMA concurred in principle with this recommendation. Although FEMA is correct in saying that the review makes no findings indicating staff did not receive appropriate training, the behavior of trained staff in this matter indicates that the training should be reviewed and improved.

Leadership Challenges in FEMA’s Mitigation Directorate

The current acting assistant administrator of the Mitigation Directorate has decades of experience in the insurance industry and the NFIP. He joined FEMA in March 1992 and worked for many years in the insurance area. In September 2008, he was appointed the acting federal insurance administrator, and as such, was the executive responsible for implementation of the new IT system. Subsequently, he was named the acting assistant administrator.

The transition of NFIP IT services from the legacy to the new contractor was troubled prior to the current acting assistant administrator’s promotion. Staff was seen as favoring either CSC or OST. NextGen was developed, accepted and paid for without testing to ensure its viability. NextGen was supposed to become the system of record in May 2008 (and then October 2008), but the transition schedule was delayed because:

- CSC and OST quarreled about data transference,
- NFIP managers did not consider NextGen capable of producing financial and actuarial reports acceptable to stakeholders, and
- NextGen did not have an Authority to Operate on FEMA’s IT network.

The acting assistant administrator admitted to knowing little about IT, the status of the transition, or IT security requirements. He relied heavily on his managers and the OST COTR to keep him informed. At various meetings from October-December 2008, the OST COTR assured the acting assistant administrator that NextGen needed minor fixes, but some managers disagreed and questioned NextGen’s ability to provide the needed financial and actuarial reports. Because of these conflicting assessments, he sought advice from a FEMA employee knowledgeable about IT. The acting assistant administrator, however, came to distrust the input he was receiving, and finally decided to seek assistance outside the Mitigation Directorate, contacting the FEMA Chief Information Officer. They were not able to meet until January 2009.

It was not until meeting with the Chief Information Officer that the acting assistant administrator learned what an Authority to Operate was, and that the legacy IT system’s Authority to Operate had expired. Additionally, he was unaware of multiple duties assigned to the OST COTR in violation of DHS IT security policy. While seeking outside IT assistance, the acting assistant administrator should have also consulted with Acquisition Management to assess whether breaches of the OST contract had occurred and how to hold OST accountable for the missed milestones.

In April 2009, the Contracting Officer told the acting assistant administrator that Acquisition Management refused to have contracts with two contractors providing parallel services. Given no alternative, the Mitigation Directorate planned to not exercise the upcoming OST contract option and notified OST accordingly. However, FEMA management intervened and instructed the Director of Acquisition Management to overrule the acting assistant administrator and continue the services of both contractors for an additional year while FEMA attempted to sort out the status of the NFIP IT transition.

Conclusion

In part due to the acting assistant administrator's overreliance on others, a critical opportunity to bring all parties together to assess the situation and determine a path forward was lost. Had the acting assistant administrator enlisted guidance from FEMA management, Acquisition Management, and the Chief Information Officer sooner, some amount of taxpayer money may have been saved.

Recommendation:

We recommend that the Administrator, Federal Emergency Management Agency:

Recommendation #4: Require the Mitigation Directorate to hire an independent, unbiased program manager to oversee the development, testing, and implementation of a new information system for the National Flood Insurance Program, including the requirements in the Statement of Work.

Management Comments and OIG Analysis

FEMA concurred in principle with this recommendation. FEMA asserts that whether an unbiased and independent program manager is hired or appointed, and to whom this person reports, needs further consideration. Any further delay in naming the program manager will be detrimental to the National Flood Insurance Program.

Appendix A
Purpose, Scope, and Methodology

FEMA asked us to conduct a review to provide suggestions for immediate improvement in the management and oversight of the NFIP's transition to a new information technology system.

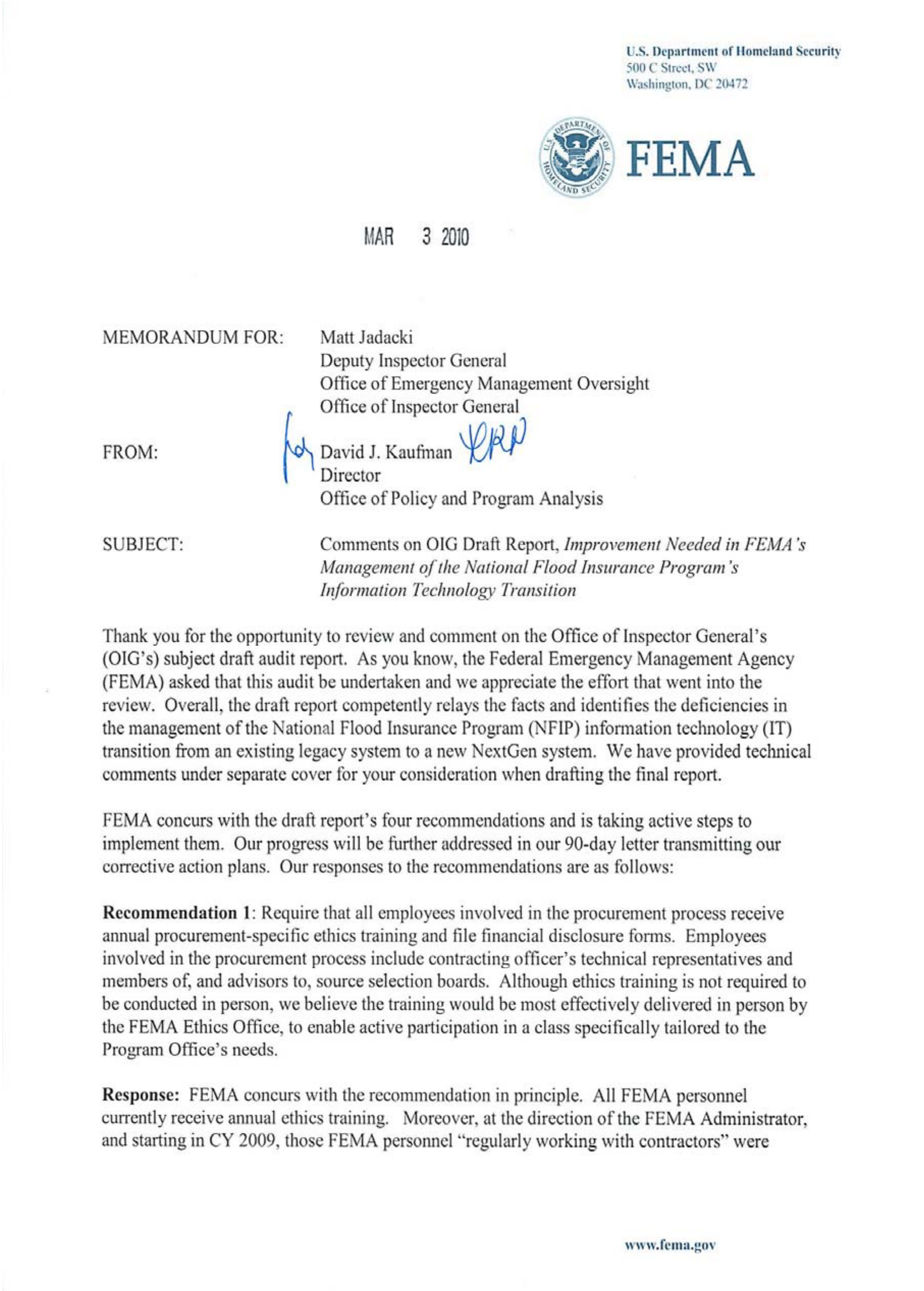
We interviewed FEMA officials and both contractors involved in the transition, and reviewed DHS and FEMA rules and regulations that were relevant to this audit. We performed fieldwork at DHS facilities in the Washington, DC area.

We began our review in July 2009 and completed it in November 2009.

We performed our work under the authority of the *Inspector General Act of 1978*, as amended, in accordance with Quality Standards for Inspections, issued by the Council of Inspectors General for Integrity and Efficiency, January 2005.

We appreciate the efforts by DHS management and staff to provide the information and access necessary to accomplish this review.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
500 C Street, SW
Washington, DC 20472

FEMA

MAR 3 2010

MEMORANDUM FOR: Matt Jadacki
Deputy Inspector General
Office of Emergency Management Oversight
Office of Inspector General

FROM: for David J. Kaufman
Director
Office of Policy and Program Analysis

SUBJECT: Comments on OIG Draft Report, *Improvement Needed in FEMA's Management of the National Flood Insurance Program's Information Technology Transition*

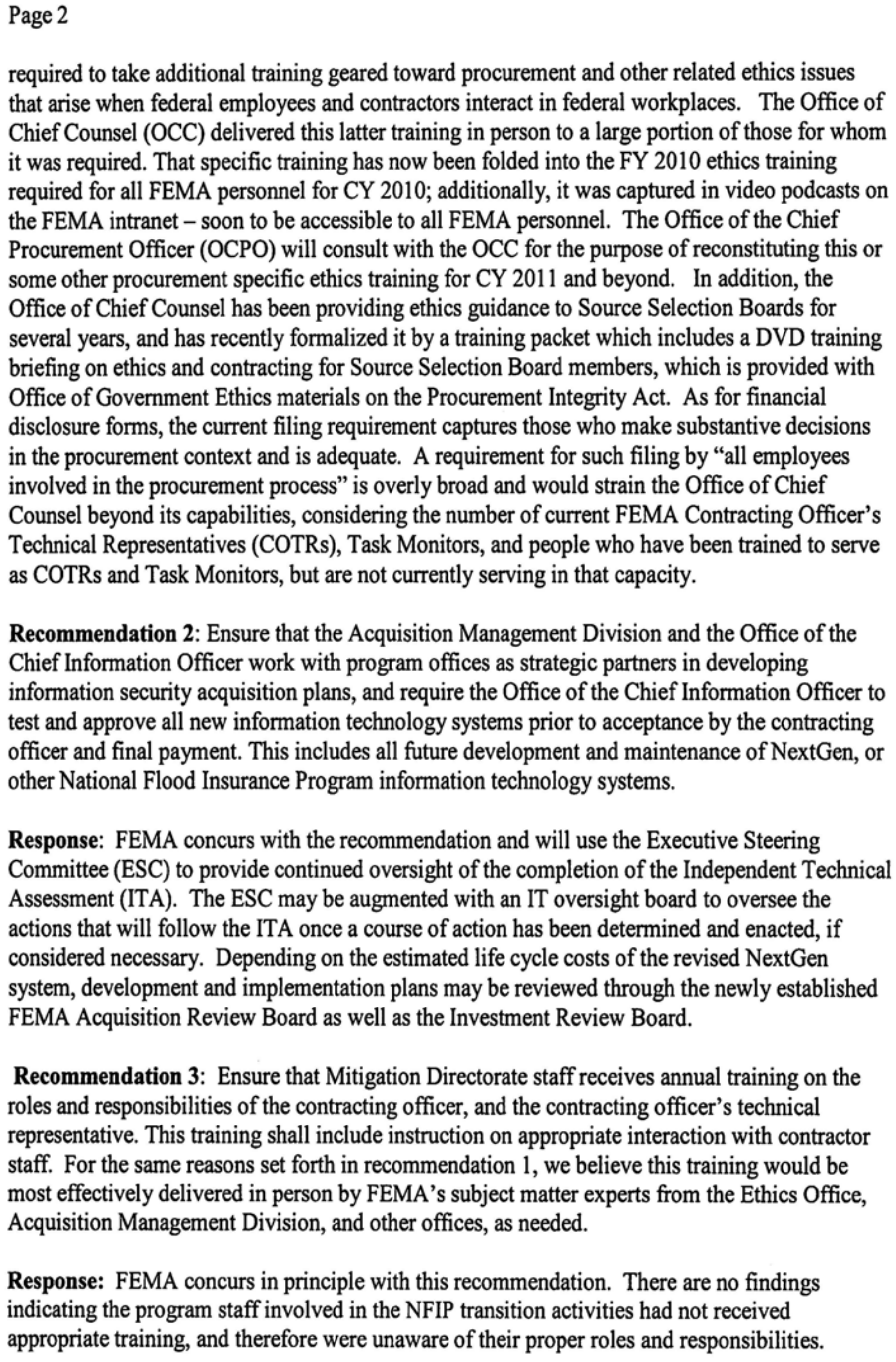
Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG's) subject draft audit report. As you know, the Federal Emergency Management Agency (FEMA) asked that this audit be undertaken and we appreciate the effort that went into the review. Overall, the draft report competently relays the facts and identifies the deficiencies in the management of the National Flood Insurance Program (NFIP) information technology (IT) transition from an existing legacy system to a new NextGen system. We have provided technical comments under separate cover for your consideration when drafting the final report.

FEMA concurs with the draft report's four recommendations and is taking active steps to implement them. Our progress will be further addressed in our 90-day letter transmitting our corrective action plans. Our responses to the recommendations are as follows:

Recommendation 1: Require that all employees involved in the procurement process receive annual procurement-specific ethics training and file financial disclosure forms. Employees involved in the procurement process include contracting officer's technical representatives and members of, and advisors to, source selection boards. Although ethics training is not required to be conducted in person, we believe the training would be most effectively delivered in person by the FEMA Ethics Office, to enable active participation in a class specifically tailored to the Program Office's needs.

Response: FEMA concurs with the recommendation in principle. All FEMA personnel currently receive annual ethics training. Moreover, at the direction of the FEMA Administrator, and starting in CY 2009, those FEMA personnel "regularly working with contractors" were

www.fema.gov



Page 2

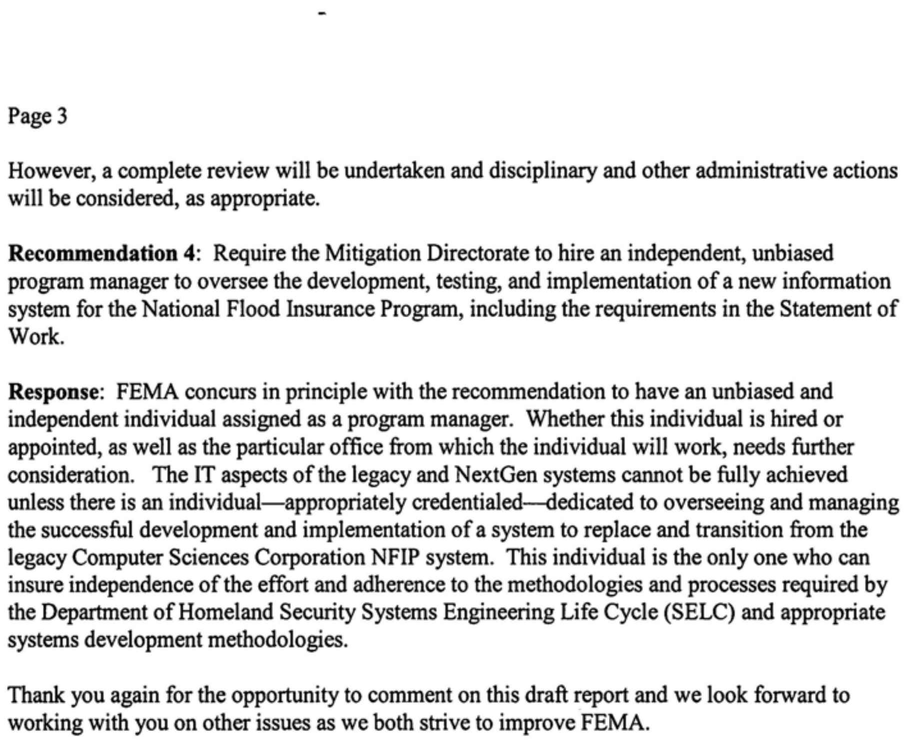
required to take additional training geared toward procurement and other related ethics issues that arise when federal employees and contractors interact in federal workplaces. The Office of Chief Counsel (OCC) delivered this latter training in person to a large portion of those for whom it was required. That specific training has now been folded into the FY 2010 ethics training required for all FEMA personnel for CY 2010; additionally, it was captured in video podcasts on the FEMA intranet – soon to be accessible to all FEMA personnel. The Office of the Chief Procurement Officer (OCPO) will consult with the OCC for the purpose of reconstituting this or some other procurement specific ethics training for CY 2011 and beyond. In addition, the Office of Chief Counsel has been providing ethics guidance to Source Selection Boards for several years, and has recently formalized it by a training packet which includes a DVD training briefing on ethics and contracting for Source Selection Board members, which is provided with Office of Government Ethics materials on the Procurement Integrity Act. As for financial disclosure forms, the current filing requirement captures those who make substantive decisions in the procurement context and is adequate. A requirement for such filing by "all employees involved in the procurement process" is overly broad and would strain the Office of Chief Counsel beyond its capabilities, considering the number of current FEMA Contracting Officer's Technical Representatives (COTRs), Task Monitors, and people who have been trained to serve as COTRs and Task Monitors, but are not currently serving in that capacity.

Recommendation 2: Ensure that the Acquisition Management Division and the Office of the Chief Information Officer work with program offices as strategic partners in developing information security acquisition plans, and require the Office of the Chief Information Officer to test and approve all new information technology systems prior to acceptance by the contracting officer and final payment. This includes all future development and maintenance of NextGen, or other National Flood Insurance Program information technology systems.

Response: FEMA concurs with the recommendation and will use the Executive Steering Committee (ESC) to provide continued oversight of the completion of the Independent Technical Assessment (ITA). The ESC may be augmented with an IT oversight board to oversee the actions that will follow the ITA once a course of action has been determined and enacted, if considered necessary. Depending on the estimated life cycle costs of the revised NextGen system, development and implementation plans may be reviewed through the newly established FEMA Acquisition Review Board as well as the Investment Review Board.

Recommendation 3: Ensure that Mitigation Directorate staff receives annual training on the roles and responsibilities of the contracting officer, and the contracting officer's technical representative. This training shall include instruction on appropriate interaction with contractor staff. For the same reasons set forth in recommendation 1, we believe this training would be most effectively delivered in person by FEMA's subject matter experts from the Ethics Office, Acquisition Management Division, and other offices, as needed.

Response: FEMA concurs in principle with this recommendation. There are no findings indicating the program staff involved in the NFIP transition activities had not received appropriate training, and therefore were unaware of their proper roles and responsibilities.



Page 3

However, a complete review will be undertaken and disciplinary and other administrative actions will be considered, as appropriate.

Recommendation 4: Require the Mitigation Directorate to hire an independent, unbiased program manager to oversee the development, testing, and implementation of a new information system for the National Flood Insurance Program, including the requirements in the Statement of Work.

Response: FEMA concurs in principle with the recommendation to have an unbiased and independent individual assigned as a program manager. Whether this individual is hired or appointed, as well as the particular office from which the individual will work, needs further consideration. The IT aspects of the legacy and NextGen systems cannot be fully achieved unless there is an individual—appropriately credentialed—dedicated to overseeing and managing the successful development and implementation of a system to replace and transition from the legacy Computer Sciences Corporation NFIP system. This individual is the only one who can insure independence of the effort and adherence to the methodologies and processes required by the Department of Homeland Security Systems Engineering Life Cycle (SELC) and appropriate systems development methodologies.

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 this Report

Donald Bumgardner, Director
Polin Cohanne, Sr. Program Analyst
Aaron Naas, Program Analyst
Trudi Powell, Audit Manager

Department Of Homeland Security
Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Chief Information Security Officer
Under Secretary for Management
FEMA Audit Liaison (10-150-EMO-FEMA)

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.