

Department of Homeland Security **Office of Inspector General**

DHS Needs To Strengthen Information Technology Continuity and Contingency Planning Capabilities

REDACTED



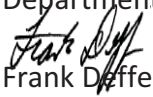


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 28, 2013

MEMORANDUM FOR: Margaret H. Graves
Acting Chief Information Officer
Department of Homeland Security

FROM: 
Frank Differ
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *DHS Needs To Strengthen Information Technology
Continuity and Contingency Planning Capabilities*

Attached for your information is our final report, *DHS Needs To Strengthen Information Technology Continuity and Contingency Planning Capabilities*. We incorporated the formal comments from the Departmental GAO/OIG Liaison Office in the final report.

The report contains nine recommendations aimed at improving the Office of the Chief Information Officer. Your office concurred with eight recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibilities under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibilities over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Division, at (202)-254-5451.

Attachment



Table of Contents

Executive Summary..... 1

Background 2

Results of Audit..... 4

 Progress Made at the Enterprise Data Centers 4

 Inadequate Continuity Planning Increases Risk That DHS May Not Be Able To
 Perform Mission Essential Functions 6

 Recommendations 9

 Inadequate Contingency Planning Increases Risk That DHS May Not Be Able To
 Restore Enterprise Mission Essential Systems 10

 Recommendations.....14

 Management Comments and OIG Analysis..... 15

Appendixes

Appendix A: Objectives, Scope, and Methodology..... 20

Appendix B: Management Comments to the Draft Report 21

Appendix C: Disaster Recovery Service Levels..... .26

Appendix D: Major Contributors to This Report 29

Appendix E: Report Distribution 30

Abbreviations

ASP	Alternate Service Provider
CBP	U.S. Customs and Border Protection
CSC	Computer Science Corporation
DC1	Enterprise Data Center 1
DC2	Enterprise Data Center 2
DHS	Department of Homeland Security
DR	disaster recovery
EMOC	Enterprise Management Operations Center



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

EOC	Enterprise Operations Center
FIPS	Federal Information Processing Standards
HP	Hewlett-Packard
IT	information technology
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OneNet	DHS One Network
OPS	Office of Operations Coordination and Planning
SOC	Security Operations Center
SP	Service Provider



Executive Summary

The Department of Homeland Security's (DHS) ability to perform mission essential functions continuously rests upon the availability and integrity of its mission essential systems and critical communications assets. We conducted an audit of the efforts undertaken by the Department's Office of the Chief Information Officer to implement and maintain continuity of operations and disaster recovery and contingency planning capabilities. The objective of our audit was to determine the progress that the Office of the Chief Information Officer has made in carrying out its continuity planning roles and developing contingency planning strategies for routine backup of critical data, programs, documentation, and personnel for recovery after an interruption.

Generally, DHS has made progress toward implementing effective disaster recovery capabilities at the Department's two enterprise data centers. Specifically, it has established a list of disaster recovery services that DHS components can procure for their systems. Additionally, the enterprise data centers now have disaster recovery enclaves that provide backup capabilities that allow continued minimum operations in the event of a disaster.

Although DHS has strengthened its disaster recovery capabilities at the Enterprise Data Centers, more work is needed. For example, the Office of the Chief Information Officer's inadequate continuity and contingency planning increases the risk that the Department may not be able to respond effectively in case of an emergency or disaster. Specifically, the Department does not have a headquarters information technology disaster recovery plan that details the transition of its headquarters critical information systems and communication assets from the primary site to the alternate site. Also, the Office of the Chief Information Officer has not established policy that requires mission essential systems to be rated as having "high" criticality in accordance with the National Institute of Standards and Technology's Federal Information Processing Standards Publication 199. Finally, because of contingency planning weaknesses, all seven of the Department's enterprise mission essential systems that we reviewed are at risk of not having capabilities to react to emergency events, to restore essential business functions if a disruption occurs, and to resume normal operations.

We are making nine recommendations to the Office of the Chief Information Officer to improve the Department's information technology continuity planning and its development of contingency strategies. The Chief Information Officer concurred with eight recommendations and has begun to take actions to implement them. The Department's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.



Background

The lessons learned from such catastrophic events as the attacks of September 11, 2001, Hurricane Katrina in 2005, and Hurricane Sandy in 2012, demonstrate the need to incorporate continuity as a good business practice into day-to-day planning, in order to reduce vulnerability and ensure resilience. An organization's resilience is the ability to resist, absorb, recover from, report, or successfully adapt to adversity or a change in conditions and is directly related to the effectiveness of its continuity capability.

On May 9, 2007, National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (National Continuity Policy) was issued to establish a comprehensive national policy on continuity for Federal Government structures and operations. National Essential Functions and continuity requirements were prescribed for all executive departments and agencies. DHS adopted the National Continuity Policy concept and has taken steps to implement it within the Department. It also has a responsibility to maintain mission essential operations for uninterrupted security and service to the United States and its citizens.

The DHS Secretary delegated to the DHS Office of Operations Coordination and Planning (OPS) responsibilities for leading and administering the Department's continuity program and Department-wide mission assurance activities. These responsibilities include developing and maintaining Department-wide continuity planning documents such as the DHS Continuity Plan, and the DHS Headquarters Continuity of Operations Plan. DHS OPS was also given the authority to ensure emergency preparedness within the Department by working, in coordination with the Under Secretary for Management and Offices and Component Heads, to ensure that plans and procedures exist for identifying, prioritizing, assessing, and protecting the Department's critical infrastructure and key resources.

OPS issued the DHS Continuity Plan to provide instructions to the Department and its components on how to continue mission essential functions during national security emergencies. The DHS Continuity Plan follows the National Security Presidential Directive-51 /Homeland Security Presidential Directive-20 and Federal Continuity Directives.¹ DHS has written the Federal Continuity Directives to provide operational

¹ The Federal Continuity Directives include Federal Continuity Directive 1—*Federal Executive Branch National Continuity Program and Requirements*, February 2008 (updated version October 2012); and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

guidance to Federal agencies on implementing the principles for the National Continuity Policy.

OPS also developed the DHS Headquarters Continuity of Operations Plan that specifies DHS policy and provides directions for the orderly relocation of headquarters personnel and continuation of headquarters essential functions at the continuity facilities, for up to 30 days, or until normal operations resume. The initiation of the Continuity of Operations Plan and procedures may be required to support any event that renders DHS operating capabilities inaccessible, unsafe, or otherwise unable to support mission requirements. The plan is important to ensure the continued performance by the Department and components in the event of a full range of potential emergencies and impactful events.

By exercising its authority, the DHS OPS assigned several key responsibilities to the Office of the Chief Information Officer (OCIO). The DHS OCIO's mission is to develop and maintain the single DHS-wide information technology (IT) infrastructure environment. DHS' IT and communication infrastructure is a crucial asset that must be strategically developed and deployed to support restoration and the continuity of operations plan in the event of man-made or natural disasters.

OCIO is responsible for the Department's mission essential function of ensuring an enterprise-level availability of IT infrastructure, mission essential systems, and communication at all levels of classification. OCIO is required to perform a business impact analysis to support its mission essential function. The OPS' Headquarters Continuity of Operations Plan defines business impact analysis as a risk method of identifying the effects of failing to perform a mission essential function or business requirement. The Headquarters Continuity of Operations Plan also directed the OCIO to develop the Headquarters IT Disaster Recovery Plan, which should include details of the transition of all DHS Headquarters Continuity of Operations Plan critical telecommunication and information systems from the Headquarters location to an alternate facility. Other key OCIO responsibilities are to identify mission essential systems and ensure the availability and integrity of the systems for use during a continuity of operations plan event. Mission essential systems include IT systems, databases, and financial management systems. A complete listing of mission essential systems should be included in the Headquarters Continuity of Operations Plan. OCIO is also responsible for informing DHS Senior Management on the status of telecommunications and information systems.

Federal Continuity Directive 2—Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, February 2008.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Contingency planning for information systems is also part of an overall organizational program for achieving continuity of operations for mission operations. Contingency planning addresses both information system restoration and implementation of alternative mission processes when systems are compromised.

We have previously reported on DHS IT contingency planning. Specifically, in May 2005, we reported that DHS IT disaster recovery sites were not prepared to prevent service disruptions.² Specifically, 15 of the 19 (79 percent) facilities reviewed did not have a recovery site or the recovery site was not fully operational. We noted that these problems with disaster recovery are occurring in part because DHS did not have a program to provide an enterprise-wide disaster recovery solution. Additionally, in April 2009, we reported that while the Department had strengthened its disaster recovery planning, more work needed to be done.³ We reported that the two new data centers need interconnecting circuits and redundant hardware for backup capabilities for each other.

Results of Audit

Progress Made at the Enterprise Data Centers

DHS has taken a number of steps to implement IT disaster recovery capabilities at the enterprise data centers since our last report in April 2009. Specifically, the OCIO established eight levels of disaster recovery capabilities for IT systems residing within the enterprise data centers. Additionally, the OCIO has set up disaster recovery enclaves to provide backup capabilities for each data center. With these enhancements to the enterprise data centers, OCIO has provided the components with additional options for disaster recovery services.

Enterprise Data Center Disaster Recovery Services

The enterprise data centers offer eight disaster recovery services levels for all component and DHS enterprise systems. From the centers, OCIO can offer components a wide range of services, including tape backups stored at offsite facilities or tape backups created using electronic vaulting services. OCIO can provide complete failover services, which is the automatic ability to move operations to a redundant backup system. For a complete list of services, see

² *Disaster Recovery Planning for DHS Information Systems Needs Improvement (Redacted)*, OIG-05-22, May 2005.

³ *DHS' Progress in Disaster Recovery Planning for Information Systems*, OIG-09-60, April 2009.



appendix C. DHS components that have information systems at either of the two enterprise data centers can procure recovery services from OCIO through the *OCIO IT Services and Hardware Catalog*, Volume 9, Summer 2012.

Enterprise Data Center Enclaves

In our April 2009 report, we noted that the enterprise data centers needed connectivity to ensure backup capabilities for each other.⁴ Specifically, we reported that the necessary telecommunications equipment and circuits were not in place to transmit data from one site to the other for backup purposes. Without the necessary connectivity between the two data centers, DHS might not be able to backup and restore mission critical systems within users' required time frames.

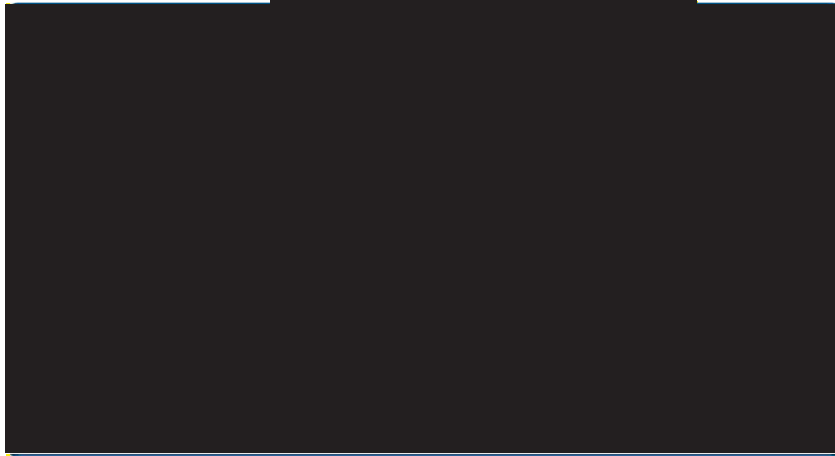
To address this issue, DHS established the disaster recovery (DR) enclaves. These enclaves are composed of

[REDACTED]

⁴ *ibid.*



Figure 1.



Inadequate Continuity Planning Increases Risk That DHS May Not Be Able To Perform Mission Essential Functions

DHS needs to conduct sufficient IT continuity planning to ensure that it can perform essential mission functions in a natural, man-made, or cyber disaster. Specifically, OCIO has not prepared a Headquarters Information Technology Disaster Recovery Plan to transition its headquarters critical information systems and communication assets from the primary location to the alternate site. Additionally, OCIO did not develop a business impact analysis to identify its mission essential function. Also, OCIO did not establish policy for the Department and components to use to identify critical information assets and mission essential systems. Finally, OCIO needs to monitor mission essential systems disaster capabilities and the usage of enterprise data center recovery services. Without adequate continuity planning, DHS is at increased risk that a catastrophic event could render the organization unable to perform mission essential functions.

Headquarters Information Technology Disaster Recovery Plan

DHS should have a Headquarters Information Technology Disaster Recovery Plan for transitioning its headquarters critical information systems and communication assets from its primary location to the alternate location during a natural, man-made, or cyber disaster. Such a plan, as required by the DHS Headquarters Continuity of Operations Plan, dated June 4, 2012, should be designed to restore operability of mission critical systems, applications, or



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

computer facility infrastructures at an alternate site after a disaster. According to an official from the DHS OCIO, OCIO has not developed a Headquarters Information Technology Disaster Recovery Plan because the OCIO currently does not have the resources to develop the plan.

An IT disaster recovery plan is a major component under continuity planning guidance. According to the National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, a disaster recovery plan is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternative site after an emergency. In a disaster recovery plan, best practices require organizations to—

- Establish a planning group with people who understand the business processes, technologies, networks and systems;
- Perform risk assessments and business impact analyses;
- Establish priority levels for business processes, applications, systems and networks;
- Develop recovery strategies; and
- Document and implement the plan.

Without a Headquarters Information Technology Disaster Recovery Plan and process in place, DHS OCIO has not been able to identify the risks to its operations and mitigate the consequences to a level acceptable to senior management.

Business Impact Analysis

DHS OCIO needs to develop a business impact analysis to identify its mission essential function, which will ensure the availability of the DHS' IT infrastructure, mission critical systems, and communications assets. The business impact analysis should identify relationships, interdependencies, and mitigation strategies to support a mission essential function. According to the DHS Continuity Plan, a business impact analysis should be conducted every 2 years in accordance with the Federal Continuity Directive 2 guidelines and requirements.⁵ According to OCIO staff, they have not conducted these analyses because of resource and staffing limitations.

⁵ Federal Continuity Directive 2—*Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, February 2008.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The DHS Continuity Plan specifies that the business impact analysis is the primary method for determining and managing risk. A business impact analysis is the first source for determining resiliency and contingency planning strategies. The results of this analysis determine how critical the system is to the supported mission/business processes, what effect the loss of the system could have on the organization, and the objective of system recovery time. The business impact analysis also determines the type and frequency of backup, the need for redundancy or mirroring of data, and the type of alternate site needed to meet system recovery objectives. Without the required business impact analysis, DHS OCIO may not have an effective risk management process to identify threats and vulnerabilities that impact mission essential systems during a disaster.

Mission Essential Systems

OCIO needs to strengthen its approach to assessing and monitoring the Department's mission essential systems. Specifically, OCIO needs to ensure that all DHS mission essential systems are rated as "high" under the availability security objective in accordance with NIST Federal Information Processing Standards Publication (FIPS) 199.⁶ NIST FIPS 199 provides three systems security levels so that organizations can rate their systems high, moderate, or low. Under the high level, any loss or disruption of a mission essential system could have a severe or catastrophic effect on the Department. We determined that some DHS enterprise mission essential systems were rated at the moderate level. Because mission essential systems must, by definition, remain available during an emergency or a disaster, components should be rating them as high.

Also, DHS OCIO needs to establish and implement processes to monitor the availability of all DHS mission essential systems. According to the OCIO's Information Technology Resilience Plan dated September 13, 2012, DHS has 234 mission essential systems. The DHS Secretary has assigned the responsibility of monitoring the availability of the mission essential systems to the DHS OCIO. These responsibilities include monitoring these systems to ensure that they are available and have the necessary disaster recovery services in the event of a disaster. OCIO staff informed us they have not instituted oversight and monitoring procedures for IT disaster recovery services because of resource and staffing limitations.

⁶ NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, pages 2–3.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Data Center Disaster Recovery Services

DHS components need to make better use of the disaster recovery services that OCIO provides through its enterprise data centers. Currently, 19 out of 234 DHS mission essential systems rely on disaster recovery services provided through the enterprise data centers platform. The DHS OCIO offers eight disaster recovery services levels in its *OCIO IT Services and Hardware Catalog*, Volume 9, Summer 2012 (see appendix C). These services are available for components to purchase through OCIO for all IT systems that are located at OCIO enterprise data centers. These types of services are crucial to ensure that DHS mission essential systems are successfully maintained and restored in the event of a disaster. Without these services, there is increased risk that the services needed to maintain DHS mission essential systems may not be available in the event of a disaster.

Recommendations

We recommend that the Chief Information Officer:

Recommendation #1:

Develop a Headquarters Information Technology Disaster Recovery Plan for the transition of its headquarters critical information systems and communications assets from its primary location to the alternate location, as instructed in the DHS Continuity of Operations Plan.

Recommendation #2:

Perform a business impact analysis of the Office of the Chief Information Officer's mission essential function and update the plan every 2 years in accordance with Federal Continuity Directive 2.

Recommendation #3:

Develop policies and processes for monitoring the availability of all DHS mission essential systems.



Inadequate Contingency Planning Increases Risk That DHS May Not Be Able To Restore Enterprise Mission Essential Systems

Contingency planning is a systematic approach for identifying what can go wrong in a situation. A system owner should try to identify contingency events and be prepared with plans, strategies, and approaches for avoiding, coping with, or even exploiting them. Our audit included a review of contingency plans for seven DHS enterprise mission essential systems, which are widely used by all DHS components. These seven systems are under the control and supervision of either the DHS OCIO or the U.S. Customs and Border Protection (CBP). The enterprise mission essential systems under the direct control of the DHS OCIO are OneNet, DC1, DC2, Redundant Trusted Internet Connection, and Email as a Service. The enterprise mission essential systems under the control of CBP are the CBP NOC and the CBP SOC. We identified areas for improvement in DHS' contingency planning that may maintain the availability of these seven systems in the event of a disruption.

NIST Special Publication 800-34 provides guidance for contingency planning for all Federal information systems to mitigate risks.⁷ Specifically, DHS enterprise system owners are not—

- Updating contingency plans on a timely basis;
- Preparing business impact analyses for each system;
- Maintaining backup data;
- Identifying adequate alternate locations for these systems;
- Implementing contingency training; or
- Performing full failover contingency testing.

Without adequate contingency planning, DHS may not have sufficient capabilities to react in an emergency and restore mission essential functions. See table 1 for a summary of our analysis of DHS contingency planning weaknesses for the selected enterprise mission essential systems.

⁷ NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table 1: DHS Contingency Planning

		Contingency Planning Requirements					
		Update Contingency Plans	Prepare Business Impact Analysis	Maintain Backup Data	Identify Adequate Alternate Locations	Implement Contingency Training for Personnel	Perform Full Failover Contingency Testing
Enterprise Mission Essential Systems	OneNet	No	No	No	Yes	No	No (partial)
	DHS Redundant Trusted Internet Connection	Yes	No	No	Yes	No	No (partial)
	DC 1	Yes	Yes	Yes	Yes	No	No
	DC 2	Yes	Yes	Yes	Yes	No	No
	DHS Email as a Service	No	Yes	Yes	Yes	No	No
	NOC	No	No	No	No	No	No
	SOC	No	No	No	No	No	No

We provide further detail on DHS’ enterprise mission essential systems and its compliance with contingency planning requirements in the following sections.

Update Contingency Plans

DHS needs to update some of its enterprise mission essential systems contingency plans. DHS Sensitive Systems Policy Directive 4300A states that documented formal information system contingency plans should be reviewed, tested, and exercised at least annually and updated as necessary.⁸ We reviewed seven enterprise mission essential systems and identified four that did not have contingency plans that were revised and updated to reflect the current system information. For example, the OneNet contingency plan, dated February 2011, was approximately 18 months old at the completion of our fieldwork. In addition, the title and date on the cover page for both the NOC and SOC contingency plans were updated prior to our review but the information within the plans was incorrect and outdated. Without updated contingency plans, the DHS OCIO may not have the capability to react effectively to disruptive events.

Prepare Business Impact Analyses

DHS should develop business impact analyses for all of its enterprise mission essential systems. Specifically, four of the enterprise mission essential systems included in our audit did not have business impact analyses prepared. Most DHS

⁸ DHS Sensitive Systems Policy Directive 4300A, Version 9.1, dated July 17, 2012, Section 3.5.2.e.



mission essential functions are supported by several systems. A business impact analysis is required for each system supporting that mission essential function. Per NIST Special Publication 800-34, business impact analysis results determine how critical the system is to the supported mission essential function processes, what effect the loss of the system could have on the organization, and length of the system recovery time.⁹ An OCIO official stated that business impact analyses were not prepared because they are not required by the DHS security policy. We agree that the DHS Sensitive Systems Policy Directive 4300A does not require system business impact analyses for contingency planning; however, the policy needs to be updated to comply with NIST Special Publication 800-34 for a system-based business impact analysis. Without the information from a business impact analysis, DHS system owners could be unable to determine the type and frequency of backups, the need for redundancy or mirroring of data, or the type of alternate site needed, to meet their system recovery objectives.

Maintain Backup Data

DHS should maintain backup data for all of its enterprise mission essential systems. Specifically, four enterprise mission essential systems do not maintain data backups in a secure offsite location to allow for ready access in a contingency event. According to DHS Sensitive Systems Policy Directive 4300A data backups should be performed on systems regularly. Information security officials stated that these enterprise mission essential systems do not have backup capabilities because of limited or reduced resources, the need for storage area networks, and expired contracts. Without adequate backup capabilities, DHS may not be able to fulfill its mission in the event of a disruption.

Identify Adequate Alternate Locations

DHS has not identified adequate alternate facilities for two of its enterprise mission essential systems, NOC and SOC. Specifically, we determined that the site in Florida that DHS chose as an alternate facility for both systems is inadequate to handle the workload if the primary sites should fail. Although the Florida site is a “hot site” in that it has fully operational equipment and capacity to assume operational control, it does not have sufficient staffing to operate effectively over an extended period. According to NIST Special Publication 800-34, one of the requirements for an alternate “hot site” is that the site must be

⁹ NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, pages 15–16.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

able to handle the full workload of the primary site.¹⁰ However, CBP does not have the staffing at the alternate site to handle the workload. In past situations, the smaller staff at the Florida site had to operate on a 24x7 schedule until the Virginia site staff could recover. A normal schedule would be an 8-hour day.

Implement Contingency Training for Personnel

DHS enterprise mission essential systems owners need to implement rigorous training requirements for all personnel involved in the contingency planning process. Specifically, we determined that all personnel supporting the seven enterprise mission essential systems we reviewed did not receive training in contingency planning. According to DHS Sensitive Systems Policy Directive 4300A, the DHS Chief Information Officer should ensure that contingency training is performed in accordance with the systems availability requirements.¹¹ DHS is required to identify personnel involved with enterprise mission essential systems and train them in their respective contingency planning roles and responsibilities, and in procedures and logistics.

Perform Full Failover Contingency Testing

DHS needs to conduct full failover testing for the seven enterprise mission essential systems we reviewed. The testing demonstrates that the system can be brought to an operational condition at the designated alternate site by following the procedures and instructions described in the contingency plan. According to DHS Sensitive Systems Policy Directive 4300A, a system's recovery roles, responsibilities, procedures, and logistics in the contingency plan should be used for testing within a year prior to authorization to recover from a simulated contingency event at the alternate processing site.¹²

In lieu of full failover testing, DHS conducted tabletop exercises or partial failover exercises for the seven enterprise mission essential systems we reviewed. These exercises were not sufficient, in that they were mostly discussion-based, and did not involve deploying equipment or other resources. A more effective, full testing exercise should be designed to exercise the roles and responsibilities, procedures, and assets, such as communications, emergency notifications, and IT equipment setup. Full testing exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan

¹⁰ *Ibid.*, page 47.

¹¹ DHS Sensitive Systems Policy Directive 4300A, Version 9.1, dated July 17, 2012, Section 3.5.2.g.

¹² *Ibid.*, Section 3.5.2.f.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

elements. Without the required full testing exercises, staff might not be able to demonstrate their operational readiness for emergencies in a simulated environment.

Recommendations

We recommend that the Chief Information Officer in coordination with CBP officials:

Recommendation #4:

Update mission essential systems contingency plans regularly.

Recommendation #5:

Prepare business impact analyses for enterprise mission essential systems.

Recommendation #6:

Develop and implement a process to maintain backup data for enterprise mission essential systems.

Recommendation #7:

Identify and establish adequate alternate facilities for the NOC and SOC.

Recommendation #8:

Implement contingency training for enterprise mission essential systems.

Recommendation #9:

Perform full failover contingency testing for enterprise mission essential systems.



Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS Government Accountability Office /Office of Inspector General Liaison Office. In the comments, OCIO concurred with recommendations 1–8, and non-concurred with recommendation nine. In addition, OCIO expressed concern with several of the conclusions presented in the report.

Specifically, OCIO stated that it does not agree with our overall assessment that “inadequate continuity and contingency planning leaves the Department vulnerable in the event of an emergency.” OCIO states that it is concerned that we “did not appropriately consider the many IT disaster recovery capabilities, documentation, and testing that, when taken together, comprise a robust disaster recovery capability.” OCIO cites as examples certain IT services, such as the DHS Emergency Response Group staff, and DHS Devolution capabilities. OCIO notes that these capabilities are tested during all National Level Exercises.

We agree that we did not discuss in detail these areas, because they were not within the scope of this audit. Rather, our objective was to determine the OCIO’s progress in carrying out its continuity planning roles and developing contingency planning strategies for routine backup of critical data, programs, documentation, and personnel for recovery after an interruption. We reviewed documentation related to Continuity of Operations Plan-designated roles and responsibilities for the OCIO but not for other DHS Headquarters offices. Nonetheless, we have revised the language in this section to state that “inadequate continuity and contingency planning increases the risk” that the Department may not be able to respond effectively in case of an emergency or disaster.

OCIO also states in the comments that it disagrees with our suggestion that all DHS mission essential systems availability ratings be changed to “high,” in that this would conflict with DHS policy. We do not agree with the OCIO in this regard. We state in our report that several of the identified mission essential systems were rated at a moderate level, which would not always ensure the availability of that system during a disaster. The mission essential function of the OCIO is to ensure that mission essential systems for the Department and the components are available during a disaster. The loss or disruption of a mission essential system could severely affect DHS operations. DHS’ current policy does not require that all mission essential systems be rated as high. This policy conflicts with NIST FIPS 199 in that FIPS requires that systems be rated at the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

high level if any loss or disruption of the mission essential system could have a severe or catastrophic effect on an agency's operations.

Finally, OCIO states that the contingency planning section of the draft report does not accurately portray the Department's contingency planning activity. According to the OCIO, the report "indicates gaps in contingency plans, business impact analyses, backup data, alternative location, training, and failover testing that are not fully accurate." For example, the OCIO states that we "did not recognize any of the contingency training performed for each of the seven systems reviewed and did not credit DHS for the robust backup capabilities of several of the systems."

We do not agree that this section of the report is inaccurate. During this audit, we reviewed contingency plans for seven DHS enterprise mission essential systems managed by the OCIO and/or CBP. We did not review contingency plans for the entire Department. Table 1, DHS Contingency Planning, presents the results of our audit based on our review of the seven enterprise systems, using DHS and NIST requirements as criteria. During the audit, we requested supporting evidence of employees' contingency training, but we only received two certificates. DHS should train their personnel in their contingency roles and responsibilities with respect to their information systems. Also, we found that four enterprise mission essential systems did not maintain back up data at secure off-site locations due to limited resources and expired contracts. DHS systems owners should establish alternate storage sites including the necessary agreements to permit the storage and recovery of information system backup information.

Our analysis of OCIO's response to our recommendations follows.

Recommendation #1

The OCIO concurs with this recommendation. The OCIO will consolidate information from the disaster recovery planning efforts and documents that already exist into one Headquarters IT Disaster Recovery Plan. Specifically, the OCIO stated that the following documents will be leveraged to develop the IT DR Plan: OCIO and DHS Headquarters Continuity of Operations Plans, the DHS Resilience Plan, and the Management Directorate Devolution Plan with Component Annex Plans.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

This recommendation will remain open until the OCIO provides documentation to support that all planned corrective actions are completed.

Recommendation #2

The OCIO concurs with this recommendation. The OCIO will coordinate with OPS to update the business impact analysis every 2 years. We agree that the steps OCIO has taken and plans to take will begin to satisfy this recommendation. This recommendation will remain open until the OCIO provides documentation to support that all planned corrective actions are completed.

Recommendation #3

The OCIO concurs with this recommendation. The OCIO agrees that policies and processes should be developed that cover automated monitoring capabilities. The OCIO will acquire services to implement automated monitoring capabilities and plans to begin system implementation this fiscal year. OCIO will develop standard operating procedures that cover the newly established monitoring capability.

We agree that the steps OCIO has taken and plans to take will begin to satisfy this recommendation. This recommendation will remain open until the OCIO provides documentation to support that all planned corrective actions are completed.

Recommendation # 4

The OCIO concurs with this recommendation. The OCIO will take steps to ensure that the enterprise mission essential systems contingency plans are updated timely on a continuing basis.

We agree that the steps OCIO has taken and plans to take will begin to satisfy this recommendation. This recommendation will remain open until the OCIO provides documentation to support that all planned corrective actions are completed.



Recommendation #5

The OCIO concurs with this recommendation. The OCIO will direct the systems owners for the cited four enterprise mission essential systems to perform business impact analyses.

We agree that the steps OCIO has taken and plans to take will begin to satisfy this recommendation. This recommendation will remain open until the OCIO provides documentation to support that all corrective actions are completed.

Recommendation #6

The OCIO concurs with this recommendation. The OCIO agrees that maintaining backup data for enterprise mission essential systems is important. They cited other methods of how data are being maintained in lieu of secure offsite location storage arrangements. This recommendation will remain open until the OCIO provides documentation to support that all corrective actions are complete.

Recommendation #7

The OCIO concurs with this recommendation. In the response, the OCIO states that they have already identified, established, equipped, staffed, and tested an adequate alternate site for the NOC and SOC.

We do not agree that the staffing levels at the NOC and SOC are adequate to handle the workload during a contingency event if the primary sites should fail. An alternative location should provide the capabilities of replicating and restoring critical applications and functions in order to resume operations in the event of an emergency. This recommendation will remain open until the OCIO provides a corrective action plan that will address the recommendation.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation #8

The OCIO concurs with this recommendation. The OCIO acknowledged that documentation to reflect training was not provided to us until after the issuance of our audit report. This recommendation will remain open until the OCIO provides documentation to support that all corrective actions are completed.

Recommendation #9

The OCIO does not concur with this recommendation. Although the OCIO agrees with the importance of performing failover contingency testing for enterprise mission essential systems, the OCIO stated that the owner of a mission essential system determines the outage risk and economics of building a fully redundant system. According to the OCIO, if it has been determined that the mission essential system requires full redundancy, the owners procure and implement a robust disaster recovery capability. When it is determined that it is not necessary for their respective systems to be fully redundant, the owners list the system as the top priority for restoration when outages occur, to mitigate risk.

We do not agree with the OCIO's comments on this recommendation. During the audit, OCIO did not provide evidence that mission essential systems owners had conducted the required analyses to determine risk and identify redundancy needs. Rather, OCIO provided documentation of the tabletop exercises that had been conducted. These exercises were not sufficient, in that they were mostly discussion-based, and did not involve deploying equipment or other resources.

According to DHS Sensitive Systems Policy Directive 4300A, a system's recovery roles, responsibilities, procedures, and logistics in the contingency plan should be used for testing, within a year prior to authorization, to recover from a simulated contingency event at the alternate processing site. Additionally, DHS has a prescribed exceptions policy through which components may request waivers to any portion of the DHS Policy Directive. During the audit, OCIO did not provide evidence that it had waived failover contingency testing for either its systems or components systems.

This recommendation will remain open until the OCIO provides documentation to support that all corrective actions are completed.



Appendix A

Objectives, Scope, and Methodology

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.

The objective of our audit was to determine the Office of the Chief Information Officer's progress in carrying out its continuity planning roles and developing contingency planning strategies for routine backup of critical data, programs, documentation, and personnel for recovery after an interruption. Specifically, we determined (1) whether disaster recovery and Continuity of Operations Plan capabilities are being used by the DHS departments and components effectively; (2) whether DHS established effective disaster recovery and Continuity of Operations Plan capabilities across selected enterprise systems; and (3) whether any recent disruptions of services have occurred and to what extent did the disruption impact components' operations.

We interviewed selected personnel at DHS Headquarters and components' facilities in Washington, DC; Clarksville, VA; and Stennis Space Center, MS.

We conducted this performance audit between August and December 2012 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Report

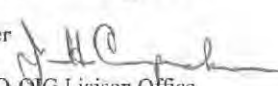
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

June 24, 2013

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumacker 
Director
Departmental GAO-OIG Liaison Office

SUBJECT: OIG Draft Report: "DHS Needs to Strengthen Information
Technology Continuity and Contingency Planning Capabilities"
(Project No. OIG-12-164-ITA-DHS)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

DHS is pleased to note OIG's acknowledgement that the Department has made progress toward implementing effective disaster recovery capabilities at the data centers. However, the DHS Office of the Chief Information Officer (OCIO) does not agree with the OIG's overall assessment that "...inadequate continuity and contingency planning leaves the Department vulnerable in the event of an emergency." OCIO is concerned that OIG apparently did not appropriately consider the many information technology (IT) disaster recovery capabilities, documentation, and testing, that when taken together, comprise a robust disaster recovery capability that has proven itself repeatedly during several recent disaster events. For example:

- OCIO, in cooperation with the DHS Office of Operations Coordination and Planning (OPS), has established continuously operable IT services and a permanent IT support team at its alternate site.
- OPS has also established back-up capability for the) at the Headquarters (HQ) alternate site for use in times of emergency or primary system failure.
- A well-established Emergency Response Group staff (ERG) also is available to activate alternate systems with detailed and documented procedures.
- The Management Directorate (MGMT) has established and documented comprehensive devolution capabilities, which include IT services, in partnership with Components, as secondary alternate sites, if the primary alternate facility is not available for any reason.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

These capabilities are tested, most notably during all annual National Level Exercises (NLEs)¹, as well as during special events. The capabilities were made known to the OIG audit team during the course of the audit and represent sound continuity and contingency planning, as well as demonstrable operational testing of an HQ IT disaster recovery capability.

OCIO also disagrees with OIG's suggestion that all DHS Mission Essential Systems (MESs) availability ratings should be changed to "high" despite the results of the assessment that the systems performed in accordance with National Institute of Standards and Technology, Federal Information Processing Standard- (FIPS-) 199 instructions. It also is important to note that the OIG's suggestion conflicts with DHS policy. Specifically, DHS Sensitive System Policy Directive 4300A requires that FIPS-199 be used to determine the sensitivity level for confidentiality, integrity, and availability of the system as the first step in authorizing an IT system. The DHS policy clearly identifies the degree of contingency capability that is required on the basis of the rating determined by completing the FIPS assessment.

Beyond DHS's current sensitive system policy, OCIO has undertaken a robust and documented effort to identify MESs, and having developed an MES list and accompanying list maintenance processes, is reconciling MES information with system accreditation records. The MES list was developed to aid in reporting and monitoring the health of DHS-wide IT services, and listing systems without a "High Availability" rating on the MES list does not necessarily represent a policy shortcoming. For a given system, justifiable criteria exist in the form of accepted recovery time/point objectives that do not warrant the investment in contingency capabilities that a formal High Availability rating implies.

The contingency planning section of the draft report also does not accurately portray the Department's comprehensive contingency planning activity. The report indicates gaps in contingency plans, Business Impact Analysis (BIA), back-up data, alternate location, training, and failover testing that are not fully accurate. For example, OIG did not recognize any of the contingency training performed for each of the seven systems reviewed and did not credit DHS for the robust back-up capabilities of several of the systems.

The draft report contained nine recommendations, eight with which the Department concurs and one with which it non-concurs. Specifically, OIG recommended that the DHS Chief Information Officer:

Recommendation 1: Develop a Headquarters Information Technology Disaster Recovery Plan for the transition of its headquarters critical information systems and communications assets from its primary location to the alternate location, as instructed in the DHS Continuity of Operations Plan.

Response: Concur. OCIO will consolidate information from the extensive disaster recovery planning efforts and documents that already exist into one HQ IT Disaster Recovery (DR) Plan. Specifically, the following existing documents will be leveraged to develop the DR Plan: OCIO and DHS HQ Continuity of Operations Plans, the DHS Resilience Plan, the MGMT Devolution Plan with Component Annex Plans, and various Concept of Operations and training

¹ NLEs are congressionally mandated preparedness exercises designed to educate and prepare participants for potential catastrophic events.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

documentation that were provided to OIG during the course of the audit. Estimated Completion Date (ECD): March 31, 2014.

Recommendation 2: Perform a business impact analysis of the Office of the Chief Information Officer's mission essential function and update it every 2 years in accordance with Federal Continuity Directive 2.

Response: Concur. OCIO will coordinate with OPS to update the business impact analysis of OCIO's mission essential function every 2 years in accordance with Federal Continuity Directive 2. ECD: June 30, 2014.

Recommendation 3: Develop policies and processes for monitoring the availability of all DHS mission essential systems.

Response: Concur. Monitoring is being performed at the Component level and by service providers for MES. OCIO agrees, however, that policies and processes should be developed that cover automated monitoring capabilities. The IT Services Office of OCIO is presently acquiring services to implement automated monitoring capabilities and plans to begin system implementation no later than September 30, 2013. OCIO will develop standard operating procedures that cover the newly established monitoring capability. ECD: December 31, 2013.

Recommendation 4: Update mission essential systems contingency plans regularly.

Response: Concur. MES contingency plans are updated annually within DHS Information Assurance Compliance tools (i.e., The Trusted Agent Federal Information Security Management Act) as required by DHS IT policy 4300A. Although some plan updates were not uploaded in a timely manner, OCIO has since updated those contingency plans and will make timely updates on a continuing basis. These updated plans are now in place and are available for OIG review. We request that this recommendation be considered resolved and closed.

Recommendation 5: Prepare business impact analyses for enterprise mission essential systems.

Response: Concur. The National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems states that the Information System Contingency Plan (ISCP) Coordinator is responsible for conducting the BIA on an information system. The ISCP Coordinator is typically a functional or resource manager within the organization. On the basis of guidance in NIST 800-34 and DHS Sensitive Systems Policy Directive 4300A, the owner of the mission essential system is responsible for conducting the BIA. The DHS CIO will direct MES owners to perform BIAs for the four MESs identified in the OIG audit as not having prepared BIAs. ECD: March 31, 2014.

Recommendation 6: Develop and implement a process to maintain back-up data for enterprise mission essential systems.

Response: Concur. OCIO argues that maintaining back-up data for enterprise mission essential systems is important and notes that a process for maintaining such data already exists.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Specifically, as recognized in the report, DHS maintains back-up data for three of the seven mission essential systems. As for the four others reviewed their data are also backed up, as appropriate, and described below.

The DHS network is a transport that does not save or store data. It is principally a service provided by two different carriers through their Multiprotocol Label Switching (MPLS) service, thus the concept of a system back-up is not applicable in the same sense as implied in the report. Back-up is accomplished through this MPLS service, which is procured with stringent service-level agreements from two carriers as a key resiliency feature. To the limited extent that the network entails Government-controlled equipment assets resident in the data centers, back-ups are regularly performed. The Network Security Plan describes the process for both the back-up plans.

Other systems similarly relies on two carriers, thus back-up concepts are also not applicable in the same sense as implied in the report. The alternate site serves as the back-up. Systems that rely more heavily on Government-controlled capabilities are resident at data centers, where back-ups are routinely performed. Given the foregoing explanation, we request that this recommendation be considered resolved and closed.

Recommendation 7: Identify and establish adequate alternate facilities.

Response: Concur. DHS has already identified, established, equipped, staffed, and tested (by virtue of active-active operation) an adequate alternate facility. The OIG was provided documentation supporting the existence of the facilities during the audit. While entirely duplicative contingency staffing at the alternate location may seem desirable, it is neither fiscally prudent nor necessary, given that current staff levels at the alternate site are adequate for immediate disaster coverage and would certainly be bolstered with staff from other locations should long-term operations at the alternate facility be required. We request that this recommendation be considered resolved and closed.

Recommendation 8: Implement contingency training for enterprise mission essential systems.

Response: Concur. DHS has implemented and is regularly performing contingency training for personnel for the seven systems reviewed in the report. Specifically, data centers have contingency training by individual job assignment and function. Other systems have contingency training provided through the TT&E (Testing, Training and Exercise) program, which provides role-based quarterly contingency training. Training has also been provided for network personnel in coordination with the NLEs as table-top exercises, as well as during the Authority to Operate process. DHS plans to continue contingency training via annual table-top exercises and in conjunction with the NLEs.

OCIO acknowledges that documentation to reflect this training was not provided to OIG until after the issuance of this draft report. In the future, OCIO will better document training events as they occur and will be able to provide related documentation in a timelier manner.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

It is important to note, Component-level system owners are directly responsible for funding the operation and maintenance of most systems in DHS. This includes provision of funds and resources for contingency training in situations where systems are dependent upon enterprise services, such as those that reside at the data centers. OCIO partners with system owners to coordinate training and other system operation and maintenance activities. We request that this recommendation be considered resolved and closed.

Recommendation 9: Perform full failover contingency testing for enterprise mission essential systems.

Response: Non-concur. The Department agrees on the importance of performing failover contingency testing for enterprise mission essential systems and has implemented failover testing as required. As proscribed by NIST guidance, the mission owner of an MES determines the outage risk and economics of building a fully redundant system. If it has been determined that the MES requires full redundancy, the mission owners have procured and implemented a robust disaster recovery capability. For those who have determined that it is not necessary for their respective MES to be fully redundant, the MES has been listed as the top priority system for restoration when outages occur to mitigate risk.

The Department tests its disaster recovery capability each year during the NLEs and system-by-system failover testing is performed periodically for all seven of the systems reviewed in this report. For example, systems hosted in one DHS data center will have an alternate data center as the failover site. Data is replicated at the alternate site in real-time. Partial failover testing was performed in October 2012, and an additional tabletop exercise was held in March 2013.

The DHS network and other systems are fully redundant, with redundant carriers, circuits, and connections. The network infrastructure is replicated at different data centers. Some of the MES reviewed run in a "live-live" configuration and are therefore failover tested whenever the other point is not reachable. We request that this recommendation be considered resolved and closed.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments regarding certain accuracy, sensitivity, context and perspective, and editorial aspects of the draft report were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.



Appendix C
Disaster Recovery Service Levels¹³

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹³ OClO IT Services and Hardware Catalog, Volume 9, Summer 2012.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹⁴ Active-Active is a phrase used to describe a network of independent processing devices where each device has access to a replicated database giving each device access and usage.



Appendix D

Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Matthews, IT Audit Manager
Beverly Dale, Team Leader
Robert Durst, Senior Program Analyst
Frederick Shappee, Program Analyst
Charles Twitty, Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
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
Under Secretary for Management
Chief Information Officer
Acting Chief Privacy Officer

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 document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

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