Department of Homeland Security
Office of Inspector General

Investigation Concerning TSA's Compromise of Covert Testing Methods

OIG-09-43

March 2009

Office of Inspector General

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

Homeland Security

March 20, 2009

Preface

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

This report summarizes the key elements of the OIG Report of Investigation regarding the Transportation Security Administration's role in the compromise of OIG's covert testing methods. It is based on interviews with employees and officials of relevant agencies and institutions, and reviews of email files and applicable documents.

We trust this report will result in more effective coordination to ensure that covert testing is not compromised in the future. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CHS	Charleston International Airport
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FSD	Federal Security Director
IED	Improvised Explosive Device
JAX	Jacksonville International Airport
OIG	Office of Inspector General
OSO	Office of Security Operations
TSA	Transportation Security Administration

Executive Summary

In response to a request from U.S. Representative Bennie Thompson, Chairman of the House Committee on Homeland Security, we investigated the events surrounding a Transportation Security Administration (TSA) email entitled "Notice of Possible Security Test." The objective of the investigation was to determine whether the email transmitted by the Assistant Administrator of TSA's Office of Security Operations compromised any covert testing by another government entity.

Our review confirmed that TSA officials compromised our covert testing methods and made no effort to report the compromise to OIG. TSA's disclosure of covert testing procedures was inappropriate and thus potentially undermined the integrity of our ongoing covert testing. We did not examine whether the email affected any other agency's covert testing because we determined that the email concerned only OIG's covert testing methods.

We are not making any recommendations. However, to improve coordination and ensure that covert testing is not compromised in future operations, we made several recommendations in our inspections report, *Transportation Security Administration's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports – Sensitive Security Information* (OIG-08-90).

Background

In November 2007, we initiated an investigation into the circumstances surrounding an email, purportedly sent by the Assistant Administrator of TSA's Office of Security Operations (OSO) on April 28, 2006, which may have compromised covert government testing of TSA airport screening checkpoints in 2006. A copy of the April 28, 2006, email is in Appendix C.

Our Office of Audits team conducted covert security testing at the Jacksonville International Airport (JAX), in Jacksonville, FL on April 27 and 28, 2006. JAX was the third airport test location in our initiative to test 14 airports nationwide during April 24 through July 14, 2006. The first airports tested were the Charleston International Airport (CHS) in Charleston, SC on April 24, 2006, and the Savannah International Airport in Savannah, GA on April 26, 2006. The covert testing we performed in 2006 tested Airport Access Control Systems, which are primarily under the control of entities within the airline industry, such as commercial airline carriers and airport authorities, not TSA.

Results of Review

TSA Compromised OIG's Covert Testing Methods

We reviewed the 2006 archived email files of multiple TSA employees associated with the release and review of the April 28, 2006, email and determined that the April 28, 2006 email provided key details about our covert airport security testing program, including our test methodology and the physical description of one of our undercover testers. We determined that airline security representatives created the email and forwarded it to TSA officials, who then broadcast the message to approximately 388 users of the TSA NetHub email system. NetHub is a division within TSA's OSO that serves as a central communications channel between TSA headquarters and TSA field operations at more than 400 airports. NetHub sends and receives communications by email, telephone, and fax on operational and administrative matters, such as distributing new screening procedures and security directives.

We interviewed the former Acting Assistant General Manager of NetHub, who stated that on April 28, 2006, he received an email from the Federal Security Director in Minneapolis-St. Paul, MN titled "TEST WARNING," which contained notices between airport directors describing tests of airport security procedures. The NetHub Acting Assistant General Manager stated that he interpreted the messages as identifying possible

unauthorized testing by nongovernment entities. The NetHub Acting Assistant General Manager said that he immediately brought the email to the Special Assistant for the Assistant Administrator of TSA's OSO and requested approval to forward the information to the field.

We determined that the message was renamed "NOTICE OF POSSIBLE SECURITY TEST" and sent from TSA's NetHub communication system on April 28, 2006, at 2:51 p.m. The email is as follows.

> "This information is provided for your situational awareness. Several airport authorities and airport police departments have recently received informal notice of possible DOT/FAA [Department of Transportation/Federal Aviation Administration] security testing at airports around the nation. Here is the text of one such notification:
>
> Several airports have reported that the DOT is testing airports throughout the country. Two individuals have been identified as FAA or DOT at the airport in JAX this morning. They have a stack of fake ID's, they try to penetrate security, place IED's [Improvised Explosive Device] on aircraft and test gate staff. These individuals were in CHS earlier this week and using a date altered boarding pass managed to get through the security checkpoint. Alert your security line vendors to be aware of subtle alterations to date info. They should also pay very close attention to the photo id's being presented. They will print a boarding pass from a flight, change the date, get through security (if not noticed) and try to board a flight and place a bag in the overhead. There is a couple, and the woman has an ID with an oriental woman's picture, even though she is Caucasian. We are getting the word out.
>
> Office of Security Operations, NetHub"

TSA Officials Made No Effort to Report the Compromise

We determined that the Assistant Administrator of TSA's OSO did not approve the April 28, 2006, NetHub email message broadcast, and actually took steps to recall it within 14 minutes. However, he did not notify us of the compromise, potentially undermining the integrity of ongoing covert testing at 11 additional airports. We also determined that several other senior TSA officials, including TSA's liaison to our covert testing team, knew about the email, but did not notify us of the compromise.

TSA responded that it has an excellent track record of cooperation with our office and with the Government Accountability Office in relation to covert testing by those offices. Further, TSA said that we and the Government Accountability Office have tested TSA operations on a regular basis for the past 5 years without any evidence of TSA employees compromising test integrity.

Our investigation confirmed that TSA officials sent the email advising its Federal Security Directors and others of covert government airport testing. The email revealed details about our testing methodology and provided tester descriptions that compromised testing procedures. The fact that the Assistant Administrator recalled the message is evidence that TSA officials considered it to be inappropriate and not an indication of unauthorized testing by nongovernment entities as initially interpreted. Further, there is no record of any attempt by TSA personnel to notify any appropriate law enforcement agency, including divisions within TSA, that unknown individuals were testing airport security.

TSA's disclosure of our covert testing procedures was inappropriate and interfered with a legitimate function of our office. In addition, at no time did any TSA official inform us that our testing was compromised.

Only Airport Police and TSA Federal Security Directors Should Be Provided Advanced Notification of Covert Testing

In addition to our investigation into the origins, creation, and dissemination of the April 28, 2006, email, we assessed the notification procedures used by TSA when its Office of Inspection conducts internal covert testing. We also reviewed our own notification procedures for possible shortfalls, and to avoid future compromises.

According to TSA's covert testing protocols, testers make appropriate notifications immediately before initiating a covert test. This notification is a necessary precaution intended to ensure the safety of the testers. During this notification, the covert testers may also solicit any areas of concern or special considerations that could arise with respect to testing. The protocols also note that the TSA managers or supervisors are not to be notified of the test.

The purpose of covert testing is to discreetly evaluate the performance of an airport under all circumstances. Those who are intent on circumventing the screening process seek to exploit any weakness and will look to take advantage of periods when the system is under tremendous stress, whether during such special circumstances or during personnel, mechanical, weather-related, or procedural difficulties.

Although we use different protocols than TSA's Office of Inspection, we have determined that we will continue our practice of advance notification. Specifically, we believe it prudent to continue providing the Federal Security Directors with advance notification of our covert testing because we are not a part of TSA's internal reporting structure and want to afford the directors this courtesy in an effort to avoid potential conflicts with airport operations. However, TSA should afford us the same courtesy it requests of its Federal Security Directors to refrain from notifying TSA managers or supervisors of covert testing. Providing advanced notification not only distorts testing results, but also negates those results as a point of comparison among airports. Such compromises prevent OIG and TSA's Office of Inspection from accurately assessing TSA's safety and security posture.

Management Comments and OIG Analysis

We received written comments on the draft letter report from TSA and have included a copy of those comments in Appendix B. We reviewed TSA's comments and made changes to our report where appropriate.

Listed below are summaries of key points made by TSA in response to findings presented in our draft report, along with OIG's analysis.

TSA Response: TSA strongly disagrees that the OIG's covert testing operations were compromised by either TSA's transmission of the NetHub email or by TSA's not reporting the occurrence to OIG. TSA states that there is no evidence that the release of the message on the NetHub system compromised covert testing and that OIG is incorrect to assert that the email revealed key details of OIG's April 2006 covert tests.

OIG Analysis: The TSA email disclosed specific details of the physical description of the testers and the testing methodology being used in 2006 for then ongoing covert tests. Additionally, TSA did not notify OIG of the email that disclosed details of our testing procedures and methods, denying us the opportunity to change our methods or personnel to ensure valid testing at the remaining 11 airports. In fact, our investigation determined that the email was received by at least four TSA officials stationed at three of the airports scheduled to be tested after JAX. Therefore, it is our position that OIG's testing methods were compromised, and, at a minimum, TSA is complicit in the compromise.

TSA Response: TSA asserts that"[i]f the transmission of [the email's contents] compromised the testing as has been alleged, OIG's April 2006 tests were compromised by the airport law enforcement community prior to TSA receiving the message." Additionally, TSA opines that "facts determined by OIG's investigation of purported tip-offs to its own covert testing exonerate TSA personnel from the allegation."

OIG Analysis: Even though the email's contents originated from a non-TSA source, TSA changed the subject line to "Notice of Possible Security Test" and forwarded the notification to 388 TSA employees. The message contained detailed information about ongoing covert government testing and was received by at least 187 TSA employees despite an email recall. Four of those employees were stationed at airports scheduled to be tested. TSA personnel took no steps to provide a follow-up explanation to the email's recipients, nor did TSA notify OIG of the compromise. Therefore, at a minimum TSA personnel were complicit in the compromise.

TSA Response: TSA also presented a list of six assertions characterized as "salient facts" which OIG addresses in turn, below.

1. *OIG conducted covert tests of airports – not TSA operations.*

   OIG Analysis: Prior to testing, OIG staff thoroughly briefed TSA personnel on the nature and scope of the tests. TSA understood that its screener positions would be tested as well because screening is an integral part of airport security. Given TSA's role in airport security, it is impossible to conduct airport security testing without including TSA. Even if one were to conclude that covert tests at airports do not involve TSA operations, we still question the conduct of TSA personnel who failed to report the compromised testing methods to the OIG.

2. *Airport law enforcement spread the word about covert testing, not TSA.*

   OIG Analysis: While our investigation traced the origin of the advance notice to an aviation security source, TSA participated in disseminating the advance notice by forwarding it to 388 TSA employees. The fact that the NetHub message was based on information originally and purposely disclosed first by another source does nothing to mitigate TSA's complicity in the disclosure of OIG's covert testing methods. TSA ignored its responsibilities to act in the best interests of the government and the department.

After receiving the email from airline security personnel entitled "Tests Warning," TSA should have taken affirmative action to quell the disclosure and to notify OIG that our covert testing methods had been disclosed, and therefore compromised. Instead, TSA "spread the word" by forwarding the text of that email to its field personnel in an email entitled "Notice of Possible Security Test." Although TSA attempted to recall the message 14 minutes later, our investigation determined that the recall was only partially effective because the email was read by at least 187 of the 388 intended recipients. TSA did nothing to explain the recalled message to its recipients, and again, did not inform OIG that our covert testing methods had been disclosed, and therefore compromised.

3. *The NetHub message in question came a day AFTER the law enforcement alert on covert testing.*

   OIG Analysis: As an agency within DHS, and one with whom we cooperate to provide enhanced airport security through our covert testing program, TSA must be held to a high standard. Our investigation focused on TSA's conduct with respect to the email, and not on the inappropriate conduct of the originators of the alert. TSA should have notified OIG of the inappropriate law enforcement alert immediately upon learning of it.

   Specific TSA personnel, who were briefed by OIG and who had knowledge of the covert testing, received the law enforcement alert on the same day it was sent, but did nothing to report the compromise to OIG. TSA had a responsibility to take affirmative action to stop the spread of the leak and to inform OIG so that further testing would not be compromised. Instead, TSA broadcast the reconstituted information to an even broader audience and took no action in the interests of the department, or the government as a whole.

4. *A NetHub duty officer passed on the law enforcement alert to TSA offices around the country – he did not intend it as a tip-off and had no knowledge about the true nature of the incidents being reported.*

   OIG Analysis: The NetHub message contained clear reference to tests being conducted by agencies of the U.S. Government (i.e., DOT/FAA) “testing airports throughout the country.” And that “two individuals were identified as FAA or DOT at the airport in JAX this morning.” The NetHub message was not a simple rebroadcast of the law enforcement alert that was merely

forwarded. Rather, it was a reconstituted version crafted by TSA that still included specific reference to government testing.

Even if the duty officer, as TSA suggests, had "a legitimate concern" that the described individuals were "posing as federal employees and presented a potential threat to aviation security," there is no evidence that any TSA personnel, including the NetHub duty officer, took any steps to alert law enforcement or even TSA's Intelligence section, of the suspected security threat. Rather, the NetHub message was sent to Federal Security Directors (and their staff), but not to law enforcement addressees or anyone in TSA Intelligence, the Federal Bureau of Investigation, or the Federal Air Marshal Service.

It is not credible to assume that TSA would fail to respond appropriately to a suspected threat to airport security. Instead, we conclude that TSA knew the email was a warning about authorized government testing.

5. *It was determined that the Assistant Administrator of TSA's Office of Security Operations did not approve the April 28, 2006, NetHub email message broadcast and actually took steps to recall it within 14 minutes*.

   OIG Analysis: Our investigation supports this statement. However, that does not excuse the actions of TSA or lessen its responsibility to act in the interests of the department and the government as a whole. The Assistant Administrator of TSA's OSO clearly recognized that the transmission of this message was inappropriate; his recall of the message without any explanation supports this conclusion. When the Assistant Administrator of TSA's OSO did nothing to report the advance notification to the OIG, in spite of knowing about OIG's then ongoing tests, he failed to meet his responsibilities. Similarly, knowing that the recall was only partially successful and at least 187 TSA employees, including addressees at airports scheduled to be tested, had received the email, he did nothing further to correct the error or minimize the potential effects of the disclosure on future testing.

6. *There was at no time any intent by officials at TSA to tip-off covert testing.*

   OIG Analysis: The OIG's investigation, the results of which are discussed above, does not support TSA's claim. The NetHub message was a reconstituted message to TSA employees, and not just a retransmission of a law enforcement alert about potential

unauthorized testing. The message clearly referred to testing by government agencies. Even if TSA personnel believed that the message was about unauthorized testing, they made no effort to notify the Federal Bureau of Investigation, the Federal Air Marshal Service, their own Intelligence section, or any other law enforcement entity about a potential threat to aviation security. After ordering a recall of the message, TSA personnel took no action to explain the inappropriate email to its recipients or to notify OIG of the compromise despite thorough knowledge of our then ongoing covert tests.

In response to a request from U.S. Representative Bennie Thompson, Chairman of the House Committee on Homeland Security, we investigated the events surrounding a Transportation Security Administration (TSA) email entitled "Notice of Possible Security Test." The purpose of our investigation was to determine whether the email transmitted by the Assistant Administrator of TSA's Office of Security Operations compromised any covert testing by another government entity.

We interviewed the former Acting Assistant General Manager of NetHub and other TSA officials. In addition, we examined the 2006 archived email files of multiple TSA employees associated with the release and review of the April 28, 2006, email.

We conducted our investigation from November 2007 to February 2008 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government investigation standards.

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

OCT 0 3 2008

Transportation Security Administration

INFORMATION

MEMORANDUM FOR: Richard J. Skinner
Inspector General
Department of Homeland Security

FROM: Kip Hawley
Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response to the Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Letter, "Report of Investigation Concerning TSA's Compromise of Covert Testing"

This memorandum constitutes TSA's formal response to the OIG draft letter, "Report of Investigation Concerning TSA's Compromise of Covert Testing," dated September 4, 2008.

Recommendation

TSA strongly disagrees with the Report's conclusion that Office of Inspector General (OIG) covert testing operations were compromised by either TSA's transmission of an e-mail on its NetHub system or by TSA's not reporting the occurrence to OIG. Because there is nothing to support the contention that an actual compromise occurred, TSA respectfully requests that all references of alleged "compromise" be deleted from the Report.

The facts determined by OIG's investigation of purported tip-offs to its own covert testing exonerate TSA personnel from that allegation. The OIG report should highlight those facts since there was public discussion that, if left uncorrected, undermines TSA leadership in its important security responsibilities. For months, those unfounded allegations have hung over several dedicated career public servants who have made outstanding contributions to our nation's security and, while the public may have moved on, these men of integrity and their families and co-workers have been deeply hurt by the unfair and unfounded allegations.

The salient facts are:

- OIG conducted covert tests of airports– not TSA operations;
- Airport law enforcement spread the word about covert testing, not TSA;
- The NetHub message in question came a day AFTER the law enforcement alert on covert testing;
- A NetHub duty officer passed-on the law enforcement alert to TSA offices around the country – he did not intend it as a tip-off and had no knowledge about the true nature of the incidents being reported;
- It was determined that the Assistant Administrator of TSA's Office of Security Operations did not approve the April 28, 2006, NetHub email message broadcast, and actually took steps to recall it within 14 minutes; and
- There was at no time an intent from officials at TSA to tip-off covert testing.

TSA welcomes the thoughts by OIG that TSA should have taken the extra step to contact OIG after the alert went out and several other process matters. However, the facts simply do not support any negative conclusions about TSA's commitment or actions related to covert test integrity.

The facts clear the individuals involved and, in fairness, this report should as well.

Discussion

In April 2006, OIG conducted covert testing of airport access control systems and challenge procedures in compliance with TSA requirements. These systems are controlled primarily by airport operators and not TSA. TSA operations were not being tested. As with all other covert testing, which is used by TSA to assess security vulnerabilities and not individual employee performance, there would have been no benefit to TSA employees to knowingly interfere with any such test, especially when TSA employees were not under evaluation.

On April 28, 2006, the Acting Assistant General Manager of NetHub in TSA's Office of Security Operations (OSO) received an electronic message from the FSD in Minneapolis-St. Paul, MN, relaying information from airport security and local police departments that unknown individuals were possibly conducting tests of security. These reports indicated the individuals may have been or were using fraudulent identification.

The Acting Assistant General Manager had no knowledge that an OIG covert testing operation was underway. Based upon the fact that daily intelligence and incident reports reviewed by OSO management include periodic reports about individuals "testing" security, there was a legitimate concern that the individuals described in the electronic message were posing as Federal employees and represented a potential threat to aviation security. Considering the actions of these individuals to be suspicious and seeking to alert our FSDs of a potential threat to aviation security, the Acting Assistant General Manager of NetHub sent the message in question to FSDs nationwide via NetHub

following approval from the Special Assistant to the Assistant Administrator for Security Operations.

As noted in the OIG draft letter, the Assistant Administrator for Security Operations did not have an opportunity to review or approve the message before its transmission. However, approximately 14 minutes after the message was sent, the Assistant Administrator read the message and directed that it be recalled.

There is no evidence that the release of the message on the NetHub system compromised covert testing. In fact, as is described in the Report, the source for the NetHub e-mail was local law enforcement—and their original notification, which was widely disseminated, occurred a day earlier. As OIG is aware from its investigation, the aviation community was sharing this information among its members for over 24 hours prior to it being received by TSA and shared with TSA personnel. If the transmission of this information compromised the testing as has been alleged, OIG's April 2006 tests were compromised by the airport law enforcement community prior to TSA receiving the message.

As a result, OIG's assertions that TSA's e-mail revealed key details are not correct. Identical messages had been circulating within the aviation community. The NetHub e-mail, which is printed by OIG in its entirety, contains no mention of either covert testing or OIG.

In addition to objecting to the finding that the issuance of the message constituted a "compromise," we strongly disagree with the Report's conclusion that the failure of the Assistant Administrator for Security Operations to notify OIG of the "compromise" potentially undermined the integrity of OIG's ongoing covert testing at 11 additional airports. The message was devoid of references to either OIG or covert testing and was timely recalled to rectify the incident.

Furthermore, the liaison personnel within the Office of Security Operations had limited knowledge of both OIG's testing methodology and the messages circulating in the law enforcement community. In addition, these personnel have additional responsibilities beyond those of liaison with OIG on covert testing. Although we would have preferred to make the connection between the messages and OIG's testing methodology at the time, TSA was concentrating on other operational matters, including the aftermath of a terminal shooting incident in which police officers were severely wounded and one person died at Cleveland Hopkins International Airport.

In addition, as OIG recommended in its related report, "Transportation Security Administration's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports" (OIG-08-90), TSA has made significant revisions to its incident management protocols. These revisions, which include the establishment of hub coordination centers, establish the protocol for operational communications from the front-line to TSA Headquarter through the Transportation Security Operations Center (TSOC). These changes have created a clear divide between

operational communications through TSOC and administrative communications through NetHub and will ensure that operational communications are checked for accuracy before transmission to the field.

Conclusion

In conclusion, TSA never disclosed OIG covert testing procedures, nor did TSA impact or interfere with the operations of OIG employees in any way. Unaware of any involvement by OIG in the security testing by unknown, unauthorized individuals that had been reported to them, OSO managers did their job and responded to a potential threat.

We agree with the point that if TSA knows of a compromise of OIG's covert testing, it should immediately inform OIG and will take immediate action if future compromises of OIG testing are discovered. The facts of this case do not support the Report's conclusions, but its overall point is well taken.

Appendix C
April 28, 2006, NetHub Email

-----Original Message-----
From: NETHUB
Sent: Friday, April 28, 2006 2:51 PM
To: TSA FSD; TSA DFSD; TSA AFSDS; TSA AFSD-R; TSA AFSD-LE
Cc: TSNM COMMERCIAL AIRLINES; TSNM COMMERCIAL AIRPORTS; Schear, James; Morris, Earl R; McGowan, Morris; Restovich, Mike; Tashiro, Susan; NETHUB
Subject: NOTICE OF POSSIBLE SECURITY TEST

Date: April 28, 2006

To: Federal Security Directors

From: Mike Restovich, Assistant Administrator, Office of Security Operations

Primary POC: NetHub

Secondary POC: None

Action Due Date: None

Subject: NOTICE OF POSSIBLE SECURITY TEST

This information is provided for your situational awareness. Several airport authorities and airport police departments have recently received informal notice of possible DOT/FAA security testing at airports around the nation. Here is the text of one such notification:

> Several airports have reported that the DOT is testing airports throughout the country. Two individuals have been identified as FAA or DOT at the airport in JAX this morning. They have a stack of fake ID's, they try to penetrate security, place IED's on aircraft and test gate staff.
> These individuals were in CHS earlier this week and using a date altered boarding pass managed to get through the security checkpoint. Alert your security line vendors to be aware of subtle alterations to date info. They should also pay very close attention to the photo id's being presented.They will print a boarding pass from a flight, change the date, get through security (if not noticed) and try to board a flight and place a bag in the overhead.
> There is a couple, and the woman has an ID with an oriental woman's picture, even though she is Caucasian. We are getting the word out.

Office of Security Operations, NetHub

Wayne Salzgaber, Special Agent in Charge, Office of Investigations

Department of Homeland Security

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Chief for Policy
Acting General Counsel
Executive Secretary
Assistant Secretary for Transportation Security Administration
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Director, GAO/OIG Liaison
TSA Audit Liaison

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) 254-4199, 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.