Department of Homeland Security

Office of Inspector General

DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers

OIG-14-02

October 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

October 24, 2013

MEMORANDUM FOR: The Honorable Suzanne Spaulding
Acting Under Secretary
National Protection and Programs Directorate

FROM: Charles K. Edwards
Deputy Inspector General

SUBJECT: *DHS' Efforts To Coordinate the Activities of Federal Cyber Operations Centers*

Attached for your information is our final report, *DHS' Efforts To Coordinate the Activities of Federal Cyber Operations Centers.* We incorporated your formal comments in the final report.

The report contains seven recommendations aimed at improving the effectiveness of coordinating the activities of the Federal cyber operations centers. Your office concurred with all recommendations. As prescribed by the *Department of Homeland Security Directive 077-1, Follow-Up and Resolutions for the 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. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. 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 responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Frank W. Deffer, Assistant Inspector General for Information Technology Audits, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

COOP	Continuity of Operations
CS&C	Office of Cybersecurity and Communications
CYBERCOM	Cyber Command
DC3	Defense Cyber Crime Center
DHS	Department of Homeland Security
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FY	fiscal year
I&A	Office of Intelligence and Analysis
IC-IRC	Intelligence Community – Incident Response Center
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
NCC	National Coordinating Center for Telecommunications
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
NIST	National Institute of Standards and Technology
NO&I	NCCIC Operations and Integration
NPPD	National Protection and Programs Directorate
NTOC	National Security Agency/Central Security Service Threat Operations Center
OIG	Office of Inspector General
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

We audited the National Protection and Programs Directorate's (NPPD) efforts in coordinating with cyber operations centers across the Federal Government. The recent increase in cyber attacks has triggered an expansion of security initiatives and collaboration between the Government and the private sector. The National Cybersecurity and Communications Integration Center, which is the operational arm of the Office of Cybersecurity and Communications within NPPD, is responsible for integrating cyber threat information from the five Federal cybersecurity centers and collaborating with these centers in responding to cyber security incidents that may pose a threat to the Nation.

NPPD has taken actions to coordinate and share vital cyber threat information with the five Federal cyber operations centers. For example, NPPD has established partnerships with the other centers to coordinate an effective response on cyber incidents. In addition, NPPD has increased interagency collaboration and communication through the use of liaisons and participating in regular meetings. Finally, NPPD has issued—in collaboration with the Federal Bureau of Investigation—Joint Indicator Bulletins to assist private sector partners in preventing cyber attacks and protecting intellectual property, trade secrets, and sensitive business information from exploitation and theft.

Still, the Department of Homeland Security (DHS) faces challenges in sharing cyber information among the Federal cyber operations centers. Specifically, DHS must procure cyber tools and technologies to improve its situational awareness efforts. In addition, it needs to work with its cyber operations center partners to develop a standard set of cyber incident reporting categories. Further, DHS has to address insufficient staffing levels that hinder its ability to provide continuous coverage in all mission areas in the National Cybersecurity and Communications Integration Center operations center and conduct additional technical training needed to improve staff's incident response skills. Finally, it must update the NPPD Continuity of Operations Plan, and finalize and integrate it with the Office of Cybersecurity and Communications' Continuity of Operations Plan and the National Cybersecurity and Communications Integration Center's Continuity of Operations Plan.

We are making seven recommendations to DHS to improve its coordination and collaboration with the Federal cyber operations centers across the Government. NPPD concurred with all recommendations and has begun to take actions to implement them. NPPD's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

The recent increase in cyber attacks has triggered an expansion of security initiatives and collaboration between the Government and the private sector. NPPD is primarily responsible for fulfilling DHS' National, non-law enforcement cybersecurity missions. Through the Office of Cybersecurity and Communications (CS&C), a sub-component of NPPD, the Department provides crisis management and coordination in response to steady-state and significant cyber incident response activities; coordinates and integrates information from the Federal cyber operations centers, state and local governments, and the private sector; and maintains an organization to serve as a focal point for the security of cyberspace.[1]

In October 2012, CS&C realigned its divisions to enhance the security, resiliency, and reliability of the Nation's cyber and communications infrastructure. Figure 1 illustrates the realignment of CS&C with a specific breakdown of the National Cybersecurity and Communications Integration Center's (NCCIC) component structure.

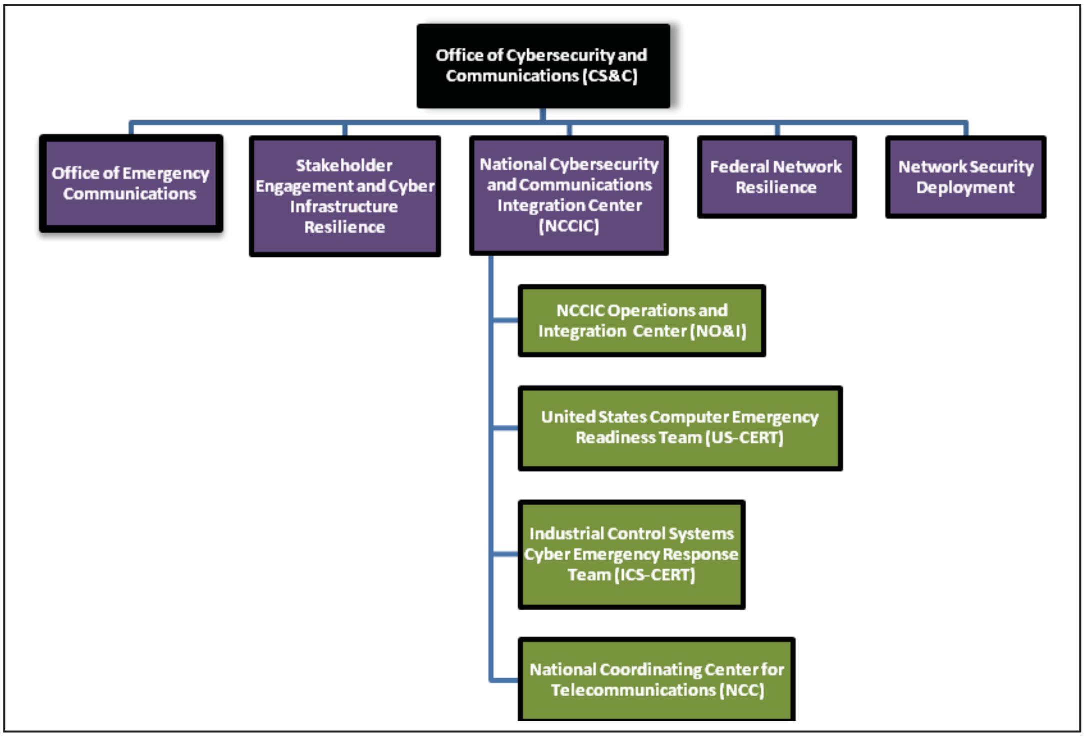

Office of Cybersecurity and Communications (CS&C)
Office of Emergency Communications
Stakeholder Engagement and Cyber Infrastructure Resilience
National Cybersecurity and Communications Integration Center (NCCIC)
Federal Network Resilience
Network Security Deployment
NCCIC Operations and Integration Center (NO&I)
United States Computer Emergency Readiness Team (US-CERT)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Coordinating Center for Telecommunications (NCC)

Figure 1: CS&C Organizational Chart

[1] A steady-state incident is an everyday cyber incident (e.g., daily intrusion and probes from sources). A significant cyber incident is a set of conditions that requires increased national coordination and may destroy, degrade, or disrupt the cyber infrastructure or integrity of the information.

The NCCIC, which is the operational arm of CS&C, coordinates national efforts and works directly with Federal, state, local, tribal and territorial governments, and private sector partners. NCCIC serves as a 24/7 centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The NCCIC comprises the following four branches:

- NCCIC Operations and Integration (NO&I)—utilizes planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident management efforts across NCCIC divisions.

- United States Computer Emergency Readiness Team (US-CERT)—identifies and analyzes suspicious activities, probable intrusions, and confirmed events, and responds to manage risk.

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)—operates in four focus areas: situational awareness for critical infrastructure and key resources stakeholders; incident response and technical analysis for control systems incidents; control systems vulnerability coordination; collaboration with other government departments and agencies to address control systems and critical infrastructure risks.

- National Coordinating Center for Telecommunications (NCC)—leads and coordinates the initiation, restoration, and reconstitution of the national security/emergency preparedness telecommunications services or facilities under all conditions.

The Comprehensive National Cybersecurity Initiative was established in 2008 to enable and support shared situational awareness and collaboration across the Federal cyber operations centers that are responsible for carrying out United States cyber activities. The need to share information on malicious activities detected on government networks between Federal cyber operations centers is vital to coordinate an effective response and have a better understanding of the threats against government information systems. For example, NCCIC communicates and shares vital cyber threat information with the following Federal cyber centers:

- United States Cyber Command (CYBERCOM), operated by the Department of Defense (DoD), establishes and maintains situational awareness and directs the operations and defense of the ".mil" networks.

- Defense Cyber Crime Center (DC3), operated by DoD, sets standards for digital evidence processing, analysis, and diagnostics for DoD investigations that require computer forensic support to detect, enhance, or recover digital media, including audio and video.

- Intelligence Community – Incident Response Center (IC-IRC), operated by the Intelligence Community, provides attack sensing and warning capabilities to characterize cyber threats and attribution of attacks and anticipates future incidents.

- National Cyber Investigative Joint Task Force (NCIJTF), operated by the Department of Justice's Federal Bureau of Investigation (FBI), serves as the multiagency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations across all national security and criminal law enforcement programs.

- National Security Agency/Central Security Service Threat Operations Center (NTOC), operated by the National Security Agency, establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity.

In September 2010, DHS developed the *National Cyber Incident Response Plan* (NCIRP) to integrate and build on current efforts to collaborate with Federal cyber operations centers and move the Nation toward a more robust common operational picture capability by integrating Federal, state, local, tribal, and territorial resources; critical infrastructure and key resources; and the private sector.[2] Effectively understanding risks in cyberspace requires that a wide range of departments, agencies, and organizations collaborate on a daily basis to identify threats, vulnerabilities, and potential consequences. The NCIRP is currently being revised by DHS based on the lessons learned from the National Level Exercise 2012 and recent cyber incidents.

Results of Audit

Actions Taken To Coordinate With Cyber Operations Centers Across the Government

NCCIC has taken several positive steps to coordinate and collaborate with Federal cyber operations centers across the Government. For example, NCCIC:

[2] A common operational picture is a single identical display of relevant operational information (i.e., network operations and monitoring, attack sensors, and cyber threat investigations) shared by multiple sources. It facilitates collaborative planning and assists all units to achieve situational awareness.

- Enhanced partnerships with other Federal cyber operations centers to respond and coordinate on specific incidents that pose a risk to the United States.

- Increased interagency collaboration and communication through the use of NCCIC liaisons, telephone calls, email, and regular meetings to leverage each organization's expertise and unique authorities to execute DHS' cybersecurity mission more effectively and efficiently.

- Collaborated with the FBI and other public and private sector partners by issuing Joint Indicator Bulletins that contain cyber threat indicators to assist network defenders in preventing cyber attacks and protecting their intellectual property, trade secrets, and sensitive business information from exploitation and theft.

- Performed functional/tabletop and no-notice (i.e., unscheduled) exercises to enhance the awareness of NCCIC's and Federal cyber operation centers' capabilities, validated plans and procedures, and coordinated relationships among partners.[3]

Although notable actions have been taken, NPPD still faces challenges in sharing cyber threat information with other Federal cyber operations centers. Specifically, NPPD can develop or procure common cyber tools and technologies, finalize and integrate CS&C and NCCIC Continuity of Operations (COOP) Plans, and provide continuous staff coverage and technical training to ensure that it can meet its critical operational mission requirements under all conditions.

Common Cyber Tools and Standardized Incident Categories Are Needed To Provide Shared Situational Awareness With Other Centers

The NCCIC and Federal cyber operations centers collectively do not have a common tool suite that can provide shared situational awareness and enhance coordinated incident management capabilities among the centers during an incident. Specifically, Federal cyber operations centers do not have a common incident management system tool that tracks, updates, shares, and coordinates cyber information with each other. Additionally, the NCCIC and Federal cyber operations centers have not standardized a set of categories for reporting

[3] The NCCIC Internal Exercise program consists of two exercise categories: functional/tabletop and no-notice. Functional/tabletop exercises are designed to engage NCCIC stakeholders or enhance partner coordination relationships. They can be conducted as a discussion-based tabletop exercise or an operations-based functional exercise. No-notice exercises are functional exercises that are unannounced to floor players. No-notice exercises are designed to train the NCCIC personnel on internal procedures.

cybersecurity incidents. Without a common incident management tool suite and standardizing security incident categorization, NCCIC and other Federal cyber operations centers will face a constant challenge in sharing cyber incident information and coordinating an effective response.

Common Cyber Tools

Currently, NCCIC relies on US-CERT's ticketing system, which is designed primarily to track the status of information technology operations, to maintain cyber incident information. US-CERT's ticketing system captures cyber incident information, such as incident occurrence and reporting dates, email correspondence between the reporting/affected agency and US-CERT, and phone conversations regarding the events. However, this ticketing system does not link situational awareness products (i.e., alerts and bulletins) that have been issued and are associated with a specific cyber incident, threat, or vulnerability. As such, incidents may not be consistently tracked, categorized, or managed seamlessly across other NCCIC components. Since NCCIC integrates cyber threat information from other Federal operations centers, having a common cyber tool will allow NCCIC to provide a comprehensive view of cyber activity across the intelligence, defense, civil, and law enforcement communities.

Federal cyber operations centers often share their information with one another. However, no single entity combines all information available from these centers and other sources to provide a continuously updated, comprehensive picture of cyber threat and network status to provide indications and warning of imminent incidents, and to support a coordinated incident response. Specifically, NCCIC does not have the tools and technologies to support continuous updates, improve efficiencies and prevent duplicative efforts in information sharing. Potential solutions include tools and technologies for incident management, shared knowledge management database, automatic call distribution and media tracking systems, dashboards, and enterprise reports for analytics which should be consolidated by the NCCIC. According to NCCIC officials, both funding and technology are needed to improve information sharing.

Further, having a common set of cyber tools will allow NCCIC to provide indicators and warning information to alert key organizations of emerging threats to the Nation's cyber infrastructure. According to the NCCIC Director, there is no national system or common cyber tool currently in place for the Federal cyber centers to share information. Additionally, the NCCIC Director acknowledged that having a common cyber tool and technology could allow the centers to provide actionable information to prevent and reduce the harm from cyber threats and vulnerabilities electronically, on a real time basis.

Standardized Cyber Incident Categories

The Federal cyber operations centers have not agreed on a standard set of categories for reporting incidents. Currently, DoD uses a 10-incident category system; DHS uses a 7-incident category system. In an attempt to standardize the incident categories, DoD developed a matrix that identifies the commonalities and differences between the DoD and DHS category systems. DoD acknowledges the need to establish common incident and event categories between DoD and DHS. Figure 2 illustrates the matrix.

DoD Cyber Incident and Reportable Cyber Event Categories	DHS Incident and Reportable Event Categories
Category 0: Training and Exercises	Category 0: Exercise/Network Defense Testing
Category 1: Root-Level Intrusions	Category 1: Unauthorized Access
Category 2: User-Level Intrusions	Category 1: Unauthorized Access
Category 3: Unsuccessful Activity Attempt	Category 5: Scans/Probes/Attempted Access
Category 4: Denial of Service	Category 2: Denial of Service
Category 5: Non-Compliance Activity	Category 4: Improper Usage
Category 6: Reconnaissance	Category 5: Scans/Probes/Attempted Access
Category 7: Malicious Code	Category 3: Malicious Code
Category 8: Investigating	Category 6: Investigation
Category 9: Explained Anomaly	

Figure 2: Matrix of DoD and DHS Incident and Events Categories[4]

Recognizing that establishing common operational terms can improve the efficiency of information sharing between Federal cyber operations centers, the IC-IRC has proposed to revise the cyber-incident categorization in the Intelligence Community. The goal of IC-IRC's effort is to serve as a first step to building a foundation for operational commonality between the centers to strengthen cyber defense. For example, IC-IRC has determined that some of the categories are not actually incident categories, but rather indications of attack vectors or investigative types. While CYBERCOM did not respond to our inquiry, DC3 and IC-IRC officials told us they have adopted the DoD's 10-incident category system. NTOC also adopted a system similar to DoD's 10-incident category system with some differences. NCIJTF officials told us that DHS' set of

[4] Source: *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B*, Appendix A to Enclosure B, Table B-A-3, dated 10 July 2012.

six Federal Agency Incident Categories does not apply to the NCIJTF or FBI because the FBI does not have a cyber defense role.

Although the DoD and DHS incident category matrix has been established, CS&C officials believe that further actions are needed. Specifically, CS&C officials are working with the National Institute of Standards and Technology (NIST) to revise the incident handling guidelines. These guidelines focus on the effect of an incident instead of how the incident happened and could be used as a national cybersecurity incident categorization system.

The *Homeland Security Act of 2002* requires DHS to establish appropriate systems, processes, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, state and local governments, and the private sector in a timely manner. Additionally, the *Cyberspace Policy Review* recommends the Federal Government develop processes between all levels of Government and the private sector to assist in preventing, detecting, and responding to cyber incidents by leveraging existing resources. Further, the Government, working with key stakeholders, should design an effective procedure to achieve a true common operating picture that integrates information from the Government and the private sector as well as serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

Developing and implementing common cyber tools and standardized incident categories are critical for monitoring, disseminating, and sharing cyber threat information among NCCIC and other Federal cyber operations centers. Having common cyber tools and technologies allow for continuously updated cyber threat information between Federal cyber operations centers and provide enhanced cross-domain situational awareness of cyber threats, vulnerabilities, and consequences, as well as a coordinated incident response. Standardization of categories would allow Federal cyber operations centers to clearly communicate incidents and events, and improve the effectiveness of information sharing activities.

Recommendations

We recommend that the Acting Under Secretary, NPPD:

Recommendation #1:

Procure or develop tools and technologies with enhanced incident management and analytical capabilities that can link situational awareness products to cyber incidents.

Recommendation #2:

Collaborate with DoD and NIST to develop a standard set of incident categories to ensure seamless information sharing between all Federal cyber operations centers.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. The Acting Under Secretary stated that NPPD and CS&C continuously work with a broad range of partners to explore new ways to enhance information sharing and deliver operationally relevant data in an efficient and effective manner. CS&C is working through its Network Security Deployment division to improve existing information sharing capabilities and bring new capabilities online as the information sharing environment matures. Release of information sharing capabilities is planned beginning in fiscal year (FY) 2014 and continuing through FY 2017. Technologies and processes to improve discoverability and availability of data between and among the cyber operations centers serve as a foundation to the information sharing capability sets. These capabilities, coupled with automated machine-to-machine data transfer, will greatly improve the ability to link data sets and improve situational awareness.

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

NPPD concurred with recommendation 2. The Acting Under Secretary stated that NPPD and CS&C have already taken decisive steps to address this recommendation as evidenced by revision two of the NIST Special Publication 800-61, published in August 2012. DHS is working with the National Security Staff and the Office of Management and Budget to release new Federal reporting guidance in the coming months. While DHS and DoD have distinct mission needs in the cyber environment, DHS will continue to work with DoD to streamline the flow of appropriate information between the two agencies.

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

Additional Staffing Can Enhance NCCIC's Ability To Provide Continuous Coverage

NCCIC's operational capabilities to respond to specific incidents may be hindered by the inability of the Office of Intelligence and Analysis (I&A) and ICS-CERT to provide their specialized functions on an around-the-clock basis. Specifically, NCCIC needs to have sufficient staffing to perform intelligence analysis functions and respond to industrial control systems incidents after work hours and on weekends. Since cyber attacks can happen at any time, it is imperative for NCCIC to have sufficient resources to respond to and mitigate potential threats.

Currently, I&A provides all-source intelligence watch and warning, operational support, and analysis and production on current, emerging, and potential threats. Additionally, I&A analysts work with NCCIC to ensure that information is incorporated with the Intelligence Community sources to provide a complete assessment of threats to the Nation. Further, I&A analysts are assigned to specific sectors based on a particular adversary's interest or activity within those sectors. However, I&A's analysts can currently provide coverage only for 14 hours per day for 5 days per week. This leaves a weekly total of 98 hours (using a 24/7basis) that I&A is not providing coverage to support the NCCIC.

ICS-CERT provides technical analysis and forensic investigations of industrial control system incidents and vulnerabilities. Additionally, these analysts provide actionable situational awareness to public and private sector partners. Currently, ICS-CERT personnel operate on a work schedule of 12 hours per day for 5 days per week. ICS-CERT does not currently have the required personnel to assist in the continuous operations of NCCIC based on current managing levels.

NCCIC management recognizes the need for additional staffing and informed us that they have requested more analysts from I&A so that NCCIC can provide more threat intelligence and analysis to all sectors under all conditions. In addition, NCCIC management indicated that they did not have funding to hire more personnel to respond to incidents regarding industrial control systems during high operational periods. Finally, NCCIC management added that they had also requested additional resources to provide more timely responses to stakeholders.

Without additional staffing for continuous coverage, the NCCIC may not be able to perform effectively all of its assigned responsibilities and provide immediate incident response and coordination with Federal cyber operations centers. Additionally, NCCIC may experience challenges in developing and rapidly distributing cybersecurity advisories and bulletins, and directly responding to and assisting its industrial control systems partners to mitigate the threats from cyber incidents.

Recommendations

We recommend that the Acting Under Secretary, NPPD:

Recommendation #3:

Augment staffing by adding additional staffing to execute ICS-CERT mission to provide full coverage on the operations floor.

Recommendation #4:

Collaborate with I&A management to increase the number of its analysts available for continuous coverage at the NCCIC to provide more intelligence and analysis to all sectors.

Management Comments and OIG Analysis

NPPD concurred with recommendation 3. The Acting Under Secretary stated that the ICS-CERT's FY 2014 President's Budget Request includes an increase of five full time equivalents. NPPD and CS&C will continue to pursue opportunities to provide additional staffing to enhance the ICS-CERT mission.

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

NPPD concurred with recommendation 4. The Acting Under Secretary stated that I&A provides all-source intelligence watch and warning, operational support, and analysis and production on current, emerging, and potential threats to NCCIC. I&A also serves as a critical link between the NCCIC and the Intelligence Community by ensuring DHS' information requirements are met and by sharing DHS' threat information with the Intelligence Community. The Under Secretary, I&A, will continue efforts to increase staffing to the NCCIC to provide continuous coverage within the constrained budget and resource environment.

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

Specialized Training Needed

NCCIC does not have sufficient resources to provide specialized training to incident responders. Additionally, analysts need to be trained on how to use various playbooks and processes to communicate incidents to Federal cyber operations center partners. Further, NCCIC must update its training and evaluation plan to reflect the new training on qualifications standards specified in the recently revised Concept of Operations. Without providing specialized training, NCCIC analysts may not possess the full scope of skills necessary to perform their assigned incident response and mitigation duties in the event of a cybersecurity attack.

As a result of the Federal Government's sequestration of FY 2013 funds, in March 2013, NPPD suspended all training for its personnel until further notice.[5] To meet the training requirements, NPPD personnel are obtaining free training through DHS' centralized learning management system, attending local conferences, or enrolling in training courses that are provided by other Federal cyber operations centers (e.g., DC3) and the Federal Emergency Management Agency's Emergency Management Institute. However, this free training does not provide incident responders with the specialized training needed to perform their assigned functions.

Our review of selected training records between 2009 to 2013 revealed that only 10 of 22 NCCIC analysts had received technical training (e.g., security and network fundamentals, introduction to malware analysis, incident handling methodology, and introduction to the forensics process). The lack of training funds has led many analysts to rely more on personal knowledge instead of the

[5] Sequestration refers to automatic spending cuts in particular categories of Federal outlays as directed in the *Budget Control Act of 2011*. Originally set to occur in January 2013, sequestration was postponed to March 2013 by the *American Taxpayer Relief Act of 2012*.

technical training to identify, respond to, and mitigate incidents. During recent NCCIC exercises, analysts relied on personal expertise and institutional knowledge of their colleagues rather than documented processes to perform their assigned duties. In exercise after-action reports, NCCIC officials acknowledged that providing specialized training to its staff is essential for accessing and analyzing information for future cyber incident response and mitigation.

Further, our review of NCCIC's after-action reports revealed that the playbooks were underutilized by floor personnel, which resulted in limited execution of appropriate operational actions.[6] The after-action reports recommend that playbooks be included in future training and exercises to enhance incident response capability.

In February 2013, NCCIC developed a training and exercise plan that incorporated learning material for Federal cyber operation center participants. Additionally, NCCIC has recently updated its Concept of Operations and plans to update its training and exercise plan to align both documents. Further, all NCCIC sub-components are required to use the recently revised personnel qualifications standards document to ensure their personnel are properly trained to perform their assigned duties by tracking formal or operationally focused training they attend.

The Comprehensive National Cybersecurity Initiative, January 2008, Initiative #8 recommends that the Nation develop a technologically-skilled and cyber-savvy workforce to ensure a continued technical advantage and future cybersecurity. Additionally, NIST recommends security personnel be provided appropriate training to combat the latest cybersecurity threats and vulnerabilities.

By providing specialized technical training to its analysts, NCCIC will increase its personnel's knowledge in current cyber threats, risks, trends, and mitigation techniques. By leveraging the National Cybersecurity Education Office assistance, NCCIC can enhance the performance, qualifications, and skills of its analysts necessary to perform incident response and mitigation functions in the event of a cybersecurity attack.

[6] Playbooks aid analysts during active cyber attack situations. They are used to quickly determine the best actions to take when faced with a given situation. The playbooks contain the adversarial moves that analysts may expect to see and countermoves believed to be effective against those moves.

Recommendation

We recommend that the Acting Under Secretary, NPPD:

Recommendation #5:

Revise the training and exercise plan to include the new qualifications and standards specified in the Concept of Operations to ensure NCCIC personnel receive the proper training, certifications, and qualifications to perform their assigned duties.

Management Comments and OIG Analysis

NPPD concurred with recommendation 5. The Acting Under Secretary stated that NCCIC personnel participate in internally and externally hosted exercises to ensure they are fully trained on processes and procedures. NCCIC has begun to expand training opportunities for staff and will continue to do so as funding becomes available.

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

NPPD Needs To Update Its COOP Plan

NCCIC's ability to timely restore its mission-essential functions in the event of an emergency may be hindered by an outdated NPPD COOP Plan.[7] Continuity of operations planning is designed to maintain or restore business operations, including computer and cyber operations, possibly at an alternate location, in the event of an emergency or disaster. However, NPPD has not updated its COOP to reflect the October 2012 realignment. As a result, CS&C and its sub-components, including NCCIC, are relying on an outdated NPPD COOP Plan to restore mission-essential functions in the event of an emergency.

In June 2013, CS&C drafted its COOP Plan that identifies and addresses additional requirements unique to its specific functions and reflects the October 2012 realignment. Further, the CS&C COOP Plan has a functional annex that identifies NCCIC's essential functions and essential supporting activities, and

[7] The purpose of a COOP plan is to establish a set of prioritized mission and business processes that must be sustained within 12 hours and for up to 30 days should interruptions occur.

reflects the updated operational framework and capabilities of the realigned CS&C. However, CS&C's COOP Plan, which should cascade down from NPPD, is not finalized. In the event that NCCIC is required to provide continuous operations at an alternate site, the outdated NPPD COOP Plan document would not provide the specific guidance for sustaining performance.

Our review of the NPPD COOP Plan and its annexes revealed that the National Cyber Security Division, which was abolished as a result of the October 2012 realignment, has not been removed from the annex. Further, the NPPD COOP Plan does not reflect the current position of the Directorate's senior management staff in its order of succession and contains incorrect and outdated information for certain key personnel in the emergency contact list. Finally, the NPPD COOP Plan does not contain detailed risk management practices and procedures to assist organizations in accomplishing continuity objectives.

An NPPD official told us that the annual review and update to the COOP Plan is scheduled for the fourth quarter of FY 2013 and will include all subcomponents of the Directorate. Additionally, NPPD's orders of succession and associated information will be updated as required during the 2013 annual review. Further, the official told us that a business impact analysis, which is to be reviewed bi-annually, was last completed in 2009 including the assessment of risks of all NPPD subcomponents.

Further, NCCIC's revised COOP Plan has not been communicated effectively to its staff to ensure the successful restoration of its mission-essential functions. For example, the following deficiencies were identified in the after-action reports during NCCIC's March and April 2013 COOP exercises:

- Floor leadership positions were not clearly identified and communicated to all floor staff. As a result, many floor personnel appeared unsure of who had the lead for coordinating overall floor activities in response to the escalating events.

- While NCC, ICS-CERT, and US-CERT communicated well within their individual components, NCCIC officials acknowledged that cross-component information sharing, both verbal and electronic, during heightened levels of operations could be improved.

- ICS-CERT noted that they were not being consulted prior to the first dissemination of the situational alert.

Agencies are required to review their essential functions and business process analyses annually and document the date of the review and names of personnel conducting the review.[8] Additionally, organizations must incorporate any identified changes generated by new organizational programs or functions or by organizational changes to existing programs or functions. Further, organizations must revise orders of succession as necessary and distribute any revisions promptly to appropriate authorities and personnel. The directive also requires that a continuity risk assessment includes an assessment of the likelihood of threats and hazards to normal operations and public safety and their consequences. Finally, agencies are required to develop a COOP plan.[9]

A current and well-tested COOP plan can ensure the recovery of mission essential functions should interruptions occur. Finalizing CS&C's COOP Plan will allow NCCIC to respond appropriately to cyber-related incidents by implementing additional requirements unique to their specific functions. Finally, testing outdated plans may create a false sense of ability to recover operations in a timely manner.

Recommendations

We recommend that the Acting Under Secretary, NPPD:

Recommendation #6:

Update the NPPD COOP Plan to reflect the current operational structure of its subcomponents and include a risk management process to ensure continuity plans are coordinated between subcomponents and continuity objectives are accomplished.

Recommendation #7:

Finalize CS&C's COOP Plan to reflect the recent alignment and test the plan to ensure that component personnel understand their roles in the event of emergency.

[8] Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, October 2012.

[9] National Security Presidential Directive – 51/Homeland Security Presidential Directive - 20, *National Continuity Policy*, May 2007.

Management Comments and OIG Analysis

NPPD concurred with recommendation 6. The Acting Under Secretary stated that while the plan may be technically outdated in certain aspects, NPPD does not believe there are any negative impacts associated with the current plan. NPPD is planning to update the current COOP plan later this year. The NPPD COOP Plan has parts that are updated as required, e.g., the Orders of Succession. These Orders of Succession have their own approval documents that may not be fully incorporated into the COOP plan when updates are approved. NPPD's Office of Business Continuity and Emergency Preparedness, the office responsible for the NPPD COOP Plan, will continue its routine, recurring communication with NPPD's sub-component COOP points of contacts, ensuring minimal confusion with regard to continuity activities and the roles and responsibilities of all parties in response to all threats.

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

NPPD concurred with recommendation 7. The Acting Under Secretary stated that CS&C is in the process of finalizing its draft COOP Plan, which is projected to be completed by the end of September 2013.

We agree with the steps that NPPD has taken and plans to take to begin to satisfy this recommendation. This recommendation will remain open and unresolved until NPPD provides documentation to support that all planned 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 effort that DHS has made in coordinating cyber operations across the Federal Government. Specifically, we determined whether:

- Processes and mechanisms exist to share cyber threat information effectively among the Federal cyber operations centers for steady-state and significant cyber incidents.

- Sharing and dissemination of cyber threat information among DHS and the Federal cyber operations centers are effective.

- Proper training and sufficient resources are provided to NCCIC leadership and key personnel to perform their incident response functions.

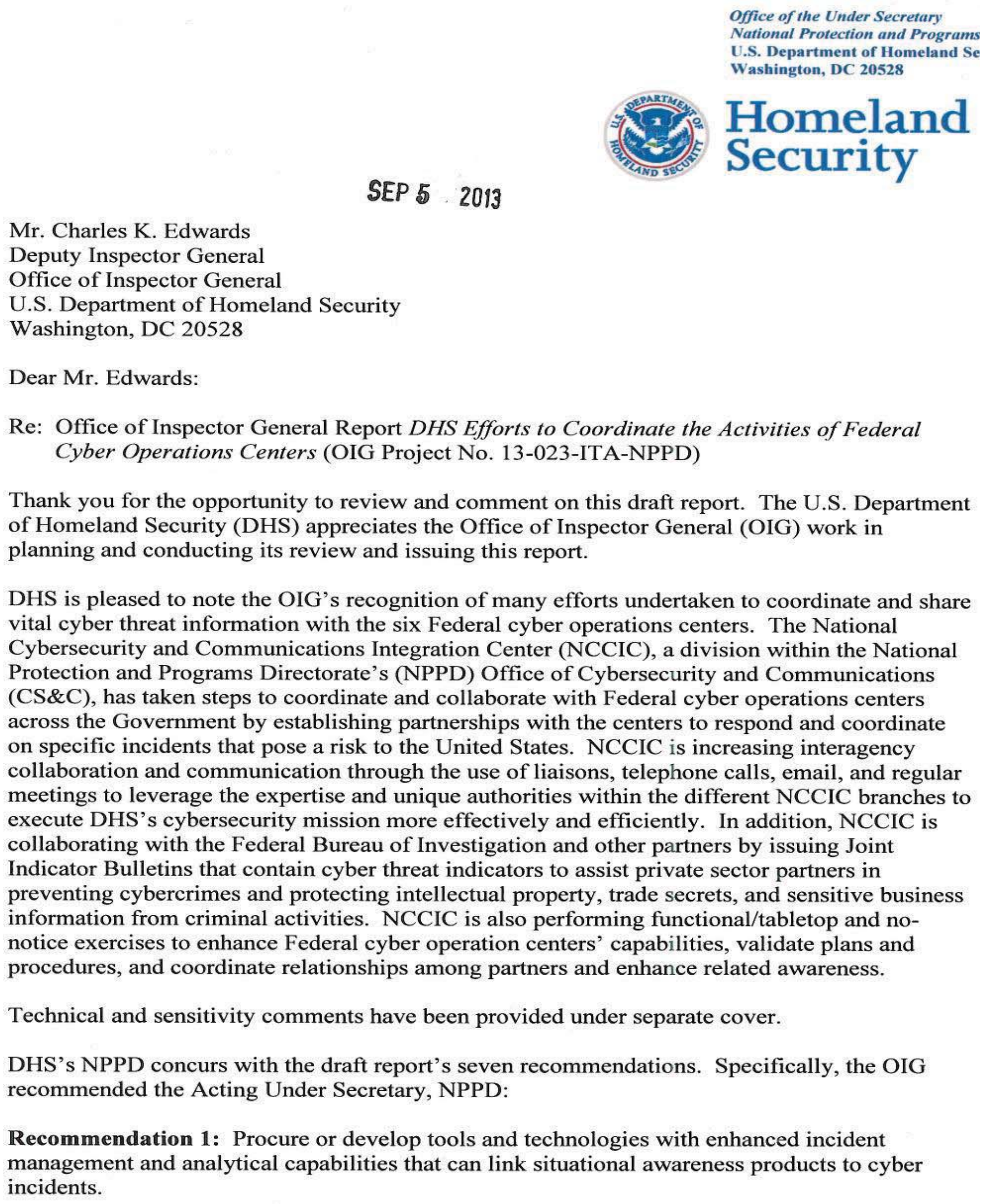
Our audit focused on NCCIC's efforts to coordinate cyber operations across the Federal Government for compliance with applicable requirements outlined in *The Homeland Security Act of 2002* and *The Comprehensive National Cybersecurity Initiative* (January 2008). We also reviewed requirements for continuity planning within National Security Presidential Directive – 51/Homeland Security Presidential Directive – 20, *National Continuity Policy* (May 2007), *National Continuity Policy Implementation Plan (August 2007)* and Federal Continuity Directive 1*, Federal Executive Branch National Continuity Program and Requirements* (October 2012).

We interviewed selected personnel from NCCIC, CS&C and NPPD, DHS Office of Chief Information Security Officer, Federal Emergency Management Agency, and I&A to discuss policy, national-level exercises, training, metrics, incident response, and information sharing. Further, we interviewed selected officials from IC-IRC, DC3, NTOC, CYBERCOM, and NCIJTF to obtain their perspective on DHS' coordination efforts with the other centers. We selected a sample of training records to determine the number of NCCIC analysts who received specialized training. In addition, we selected a sample of incident reports to evaluate the process and the system used to maintain cyber threat information. Fieldwork was performed in the Washington, DC area.

We conducted this performance audit between January 2013 and May 2013 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. Major OIG contributors to the audit are identified in appendix C.

The principal OIG point of contact for the audit is Frank W. Deffer, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4100.

Appendix B
Management Comments to the Draft Report



Office of the Under Secretary
National Protection and Programs
U.S. Department of Homeland Se
Washington, DC 20528

Homeland
Security

SEP 5 2013

Mr. Charles K. Edwards
Deputy Inspector General
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Edwards:

Re: Office of Inspector General Report *DHS Efforts to Coordinate the Activities of Federal Cyber Operations Centers* (OIG Project No. 13-023-ITA-NPPD)

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 (OIG) work in planning and conducting its review and issuing this report.

DHS is pleased to note the OIG's recognition of many efforts undertaken to coordinate and share vital cyber threat information with the six Federal cyber operations centers. The National Cybersecurity and Communications Integration Center (NCCIC), a division within the National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C), has taken steps to coordinate and collaborate with Federal cyber operations centers across the Government by establishing partnerships with the centers to respond and coordinate on specific incidents that pose a risk to the United States. NCCIC is increasing interagency collaboration and communication through the use of liaisons, telephone calls, email, and regular meetings to leverage the expertise and unique authorities within the different NCCIC branches to execute DHS's cybersecurity mission more effectively and efficiently. In addition, NCCIC is collaborating with the Federal Bureau of Investigation and other partners by issuing Joint Indicator Bulletins that contain cyber threat indicators to assist private sector partners in preventing cybercrimes and protecting intellectual property, trade secrets, and sensitive business information from criminal activities. NCCIC is also performing functional/tabletop and no-notice exercises to enhance Federal cyber operation centers' capabilities, validate plans and procedures, and coordinate relationships among partners and enhance related awareness.

Technical and sensitivity comments have been provided under separate cover.

DHS's NPPD concurs with the draft report's seven recommendations. Specifically, the OIG recommended the Acting Under Secretary, NPPD:

Recommendation 1: Procure or develop tools and technologies with enhanced incident management and analytical capabilities that can link situational awareness products to cyber incidents.

Response: Concur. NPPD and CS&C continuously work with a broad range of partners to explore new ways to enhance information sharing and deliver operationally relevant data in an efficient and effective manner. CS&C is working through its Network Security Deployment division to improve existing information sharing capabilities and bring new capabilities online as the Information Sharing environment matures. Release of Information Sharing capabilities is planned beginning in Fiscal Year (FY) 2014 and continuing through FY 2017. Technologies and processes to improve discoverability and availability of data between and among the cyber operations centers serve as a foundation to the Information Sharing capability sets (implementation stages). These capabilities, coupled with automated machine-to-machine data transfer, will greatly improve the ability to link data sets and improve situational awareness.

Recommendation 2: Collaborate with the Department of Defense (DOD) and NIST (National Institute of Standards and Technology) to develop a standard set of incident categories to ensure seamless information sharing between all Federal cyber operations centers.

Response: Concur. NPPD and CS&C have already taken decisive steps to address this recommendation as evidenced by revision two of NIST SP 800-61, published in August 2012. DHS is working with the National Security Staff and the Office of Management and Budget to release new federal reporting guidance in the coming months. While DHS and the Department of Defense (DOD) have distinct mission needs in the cyber environment, DHS will continue to work with DOD to streamline the flow of appropriate information between the two agencies.

Recommendation 3: Augment staffing shortages by adding additional staffing to execute the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) mission to provide full coverage on the operations floor.

Response: Concur. The FY 2014 President's Budget Request for the ICS-CERT includes an increase of five full time equivalents. NPPD and CS&C will continue to pursue opportunities to provide additional staffing to enhance the ICS-CERT mission.

Recommendation 4: Collaborate with I&A (Office of Intelligence and Analysis) management to increase the number of its analysts available for continuous coverage at the NCCIC to provide more intelligence and analysis to all sectors.

Response: Concur. DHS's I&A provides all-source intelligence watch and warning, operational support, and analysis and production on current, emerging, and potential threats to NCCIC. I&A also serves as a critical link between the NCCIC and the Intelligence Community (IC) by ensuring DHS information requirements are met and by sharing DHS threat information with the IC. The Under Secretary, I&A, will continue efforts to increase staffing to the NCCIC to provide continuous coverage within the constrained budget and resource environment.

Recommendation 5: Revise the training and exercise plan to include the new qualifications and standards specified in the Concept of Operations to ensure NCCIC personnel receive the proper training, certifications, and qualifications to perform their assigned duties.

Response: Concur. To ensure NCCIC personnel are fully trained on processes and procedures, NCCIC personnel participate in internally and externally hosted exercises. NCCIC has begun to expand training opportunities for staff and will continue to do so as funding becomes available.

Recommendation 6: Update the NPPD Continuity of Operations (COOP) to reflect the current operational structure of its subcomponents and include a risk management process to ensure continuity plans are coordinated between subcomponents and continuity objectives are accomplished.

Response: Concur with the recommendation that the plan be updated. While the plan may be technically outdated in certain aspects, NPPD does not believe there are any negative impacts associated with using the current plan. NPPD is planning to update the current COOP plan later this year. The NPPD COOP Plan – as is the case with all similar COOP plans – is a living document and has parts that are updated as required, e.g. the Orders of Succession. These Orders of Succession have their own approval documents that may not be fully incorporated into the COOP plan when updates are approved. NPPD's Office of Business Continuity and Emergency Preparedness, the office responsible for the NPPD COOP Plan, will continue its routine, recurring communication with NPPD's Subcomponent COOP points of contacts, ensuring minimal confusion with regard to continuity activities and the roles and responsibilities of all parties in response to all threats. Implementation of this recommendation is NPPD's responsibility as opposed to CS&C.

Recommendation 7: Finalize CS&C's COOP to reflect the recent alignment and test the plan to ensure that component personnel understand their roles in the event of emergency.

Response: Concur. Currently, CS&C is in the process of finalizing its draft COOP Plan which is projected to be completed by the end of September 2013.

We look forward to working with you on future homeland security engagements.

Sincerely,

Suzanne E. Spaulding
Acting Under Secretary

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, IT Audit Manager
Shannon Frenyea, Senior Program Analyst
Megan Ryno, Program Analyst
Sheldon Liggins, IT Auditor
Scott He, Referencer

Appendix D
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
Acting Assistant Secretary, Cybersecurity and Communications
Acting Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, National Cybersecurity and Communications Integration Center
Director, Compliance and Oversight Program, Office of Chief Information Security Office
Director of Local Affairs, Office of Intergovernmental Affairs
Audit Liaison, NPPD
Audit Liaison, DHS, Chief Information Security Office
Audit Liaison, DHS, Chief Information Officer
Audit Liaison, CS&C
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.

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.