Department of Homeland Security

Office of Inspector General

DHS Can Strengthen Its International Cybersecurity Programs (Redacted)

OIG-12-112

August 2012

Table of Contents

Appendixes

Abbreviations

CERT	Computer Emergency Response Team
CS&C	Office of Cybersecurity and Communications
DHS	Department of Homeland Security
HSPD-7	Homeland Security Presidential Directive 7
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT	information technology
[redacted]	[redacted]
NCSD	National Cyber Security Division
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
QHSR	Quadrennial Homeland Security Review
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

The borderless nature of threats to, and emanating from, cyberspace requires robust engagement and strong partnerships with countries around the world. International engagement is a key element of the Department of Homeland Security's (DHS) cyber mission to safeguard and secure cyberspace. As such, the National Protection and Programs Directorate (NPPD) has established multiple functions to support its international affairs program, which promotes cybersecurity awareness and fosters collaboration with other countries and organizations.

We determined whether NPPD has established effective programs and partnerships to collaborate and share cybersecurity information with the international community. We also evaluated whether NPPD is promoting the benefits of networked technology globally, and a secure, reliable, and interoperable cyberspace.

Overall, NPPD and its subcomponents have undertaken actions to promote collaboration with the international community and develop partnerships with other nations to better protect cyberspace. For example, NPPD and its subcomponents participate in international cyber exercises, capacity building workshops, and multilateral and bilateral engagements. The Directorate also utilizes innovative technologies to share cyber data with its partner nations.

While continuing to build upon existing partnerships, NPPD's Office of Cybersecurity and Communications needs to establish and implement a plan and goals to further its international affairs program with other countries, international industry, and the private sector to protect global cyberspace and critical infrastructure. For more efficient and effective operations, NPPD should streamline its international affairs functions to better coordinate foreign relations and consolidate resources. Finally, the United States Computer Emergency Readiness Team needs to strengthen its communications and information-sharing activities with and among its counterparts to promote international incident response and the sharing of best practices.

We are making five recommendations to the Under Secretary, NPPD. The Under Secretary, 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

Our Nation's economy and security are highly dependent on the global cyber infrastructure. Specifically, our Nation depends on a complex array of interdependent and critical networks, systems, and resources that can be disrupted from both inside and outside of the physical borders of the United States. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society. As such, the Internet has been identified as a key resource, made up of domestic and international assets within the information technology (IT) and communications sectors.

Cybersecurity involves the protective measures needed to secure cyberspace and its associated infrastructure as well as the restoration of information systems and the data contained therein. As defined, cybersecurity comprises the collection of tools, security policies, guidelines, risk management approaches, training, best practices, assurance, and technologies that can be used to protect the global information and communications infrastructure. In addition, it includes the full range of threat and vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies.

Owing to cybersecurity's borderless nature, it is essential that foreign governments and international organizations play an active role in developing cyberspace security policies and procedures aimed at improving collaboration, information sharing, and incident response capabilities. As the Internet's core functionality relies on systems of trust, the international community needs to recognize the implications of its technical decisions and act with respect for one another's networks with the broader interest of preserving global network functionality and improving security.

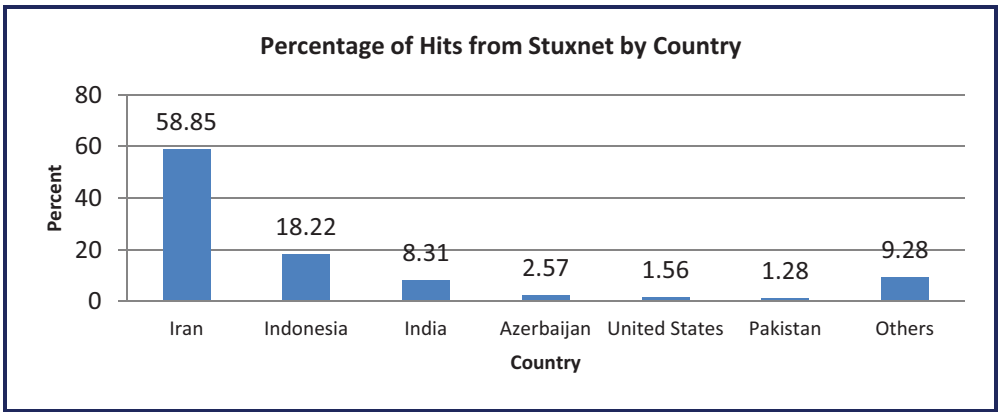
As outlined in *The National Strategy to Secure Cyberspace*, the need to secure cyberspace is a global matter due to the interconnectedness of the world's computer systems.[1] The global interconnectivity provided by the Internet allows malicious users to easily cross national borders, affect large numbers of individuals, and maintain anonymity. Different types of cyber threats may use various exploits to adversely affect computers, software, networks, agencies' operations, industries, or the Internet itself. A series of high-profile events reported since 2010 highlight the increasing and multifaceted threat of global cyber attacks:

- The Stuxnet worm targets software and equipment used in industrial control systems. It was discovered in July 2010, but may have existed at least 1 year earlier and likely

[1] *The National Strategy to Secure Cyberspace* was issued in February 2003.

even before. It was reported in August 2010 that 60 percent of the infected computers worldwide were in Iran.[2] Figure 1 shows the countries most affected by the worm.

Figure 1: Countries Affected by Stuxnet



Source: Symantec.

- In November 2011, industrial secrets from Norwegian oil, gas, energy, and defense industries were stolen through phishing attacks that were sent with viruses designed to search entire hard drives for sensitive data.

- In February 2012, the international hacking group Anonymous attacked the Swedish Government's website. The website, used by all Swedish Government departments, was brought down by overloading it with traffic.

Recognizing the challenges and opportunities inherent in securing cyberspace, the President identified cybersecurity and the establishment of related performance metrics as key management priorities of his administration. Shortly after taking office, President Obama directed a 60-day comprehensive review to assess U.S. policies and structures for cybersecurity, known as the Cyberspace Policy Review. Upon completion of the review, a report titled *Assuring a Trusted and Resilient Information and Communications Infrastructure* was issued in May 2009. The importance of securing cyberspace is also outlined in DHS' 2010 Quadrennial Homeland Security Review (QHSR), which established the first strategic framework to guide the Department's activities toward a Nation that is safe, secure, and resilient against terrorism and other hazards.

[2] Although this is not the first time hackers have targeted industrial control systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller rootkit.

To address the recommendations made in the President's Cyberspace Policy Review, the White House released the *International Strategy for Cyberspace* (*Strategy*) in May 2011. The *Strategy* outlines the Nation's approach to unify our engagement with international partners on a full range of cyber issues. It calls for the United States to work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens security, and fosters free expression and innovation to reduce the threats we face.

The *Blueprint for a Secure Future: The Cybersecurity Strategy for the Homeland Security Enterprise* (*Blueprint*), dated November 2011, builds on the QHSR framework. It provides a clear plan of action for the Department to take to implement the goals set forth in the QHSR. This strategic concept will drive the prioritization of resources and build the capabilities needed to achieve DHS' goals for protecting cyberspace, which include strong international collaboration.

DHS is responsible for leading the protection and defense of Federal civilian networks against cyber threats, and coordinating response to cyber attacks and security vulnerabilities. Homeland Security Presidential Directive – 7 (HSPD-7) directs DHS to "maintain an organization to serve as a focal point for the security of cyberspace" and to "facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations." The QHSR and the *Blueprint* serve as guides for the Department's cybersecurity mission and related international programs and initiatives.

By collaborating with foreign partners, DHS can enhance cybersecurity and fulfill its primary domestic mission. As such, international engagement is a core aspect of the missions of NPPD and its Office of Cybersecurity and Communications (CS&C). CS&C is responsible for addressing the challenges to secure cyberspace, cyber assets, and our Nation's IT infrastructure.[3] In September 2011, CS&C created a new International Affairs Program to better coordinate its international engagements. In addition, NPPD's International Affairs Coordination Program is responsible for the strategic planning and coordination of international affairs across the Directorate.

[3] The IT infrastructure consists of critical functions—sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (research and development, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.

The National Cyber Security Division (NCSD), which is a component of CS&C, is the national focal point for cybersecurity in the public and private sectors. As such, NCSD serves as the Government's lead in assessing, mitigating, and responding to cyber risks in collaboration with Federal, State, and local governments, the private sector, academia, and international partners.

NCSD is composed of five branches responsible for meeting the Department's cybersecurity mission, including the United States Computer Emergency Readiness Team (US-CERT). In mitigating potential security threats to Federal information systems, US-CERT can direct the operation and defense of Government connections to the Internet. The International Affairs Program within NCSD's Critical Infrastructure Cyber Protection and Awareness Branch is responsible for promoting cybersecurity awareness and fostering cybersecurity collaboration with international partners. Further, a number of other programs within NCSD have international engagements, including the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Global Cyber Security Management Branch, and the Cyber Exercise Program.

Results of Audit

Actions Taken To Foster Relationships With the International Community

To implement the President's *Strategy*, CS&C has taken steps to promote global cybersecurity collaboration, develop partnerships with other nations, and build technologies to help share and disseminate cyber threat and vulnerability information with its international partners. Specifically, NCSD's International Affairs Program has developed strategic objectives to promote cybersecurity awareness and foster collaboration with international partners, as outlined in the *Strategy*. Figure 2 illustrates the five strategic objectives developed for NCSD's International Affairs Program.

Figure 2: NCSD's International Strategic Objectives

Strategic Objectives
Build upon and create new relationships and structures to facilitate collaboration with international partners
Strengthen operational collaboration with international counterparts
Build capacity in areas where DHS has expertise, such as national capabilities for incident management; public/private partnerships; control systems security; and awareness raising
Cultivate and advance meaningful engagement with industry on international cybersecurity issues
Promote U.S. interagency cybersecurity goals and provide leadership and expertise in international forums.

Source: NCSD International Affairs Program

CS&C and NCSD engage in a multitude of activities and initiatives to satisfy NPPD's mission and goals, as outlined in the *Strategy*. The following actions are examples:

- NCSD serves as an active member of the [redacted], a collaborative effort among Australia, Canada, New Zealand, the United Kingdom, and the United States to improve situational awareness and share cybersecurity threat and warning information.

- As an active participant within the U.S. delegation to the Organization of American States, NCSD leads many capacity building workshops and aids in the development of national-level cybersecurity strategies and programs through discussion and sharing of best practices with member nations. For example, US-CERT representatives participated in the Organization of American States' Inter-American Committee against Terrorism cybersecurity workshop to discuss best practices for developing and implementing cybersecurity exercises on November 7–8, 2011.

- As a contributing member of the [redacted] NCSD, through US-CERT and ICS-CERT, collaborates with [redacted] partners to share cybersecurity information.[4] [redacted].

[4] [redacted].

- CS&C has developed formal and informal agreements to define its bilateral engagements, including dialogue frameworks, information sharing protocols, and levels of collaboration, as requested by specific foreign nations.

- NCSD, as a founding member of the Meridian process and an active participant of the program committee, has helped plan and taken part in the Meridian's annual conferences since their conception. Most recently, NCSD participated at the Meridian Conference in Doha, Qatar, in October 2011. The Meridian conferences provide a forum for countries to share information relating to cybersecurity initiatives, critical infrastructure protection issues, best practices, and lessons learned to improve global cybersecurity infrastructure.

- NCSD plans and participates in international cyber exercises to build upon lessons learned from previous real world incidents. For example, in November 2011, NCSD, in conjunction with its European colleagues, planned and executed the first joint European Union-United States table top exercise, Cyber Atlantic 2011, in which 17 countries participated.

- CS&C and NCSD participate in the Information Technology Sector Coordinating Council's International Committee meetings to discuss cybersecurity initiatives and promote cooperation with the private sector on international issues. Membership consists of representatives from private industry.

Although CS&C has taken actions to develop partnerships with other nations and promote global cybersecurity collaboration, it can take additional steps to better protect global cyberspace. Specifically, CS&C must fully develop its policies and procedures, streamline its international affairs programs, and improve communications and information sharing with foreign nations to better meet NPPD's cybersecurity mission and goals.

CS&C Has Not Developed a Strategic Implementation Plan for Foreign Engagement

CS&C has not yet developed a strategic implementation plan that outlines its responsibilities or establishes specific timeframes and milestones to provide a clear plan of action for achieving its cybersecurity goals with international partners. In addition, CS&C has not defined its roles for carrying out the mission of its International Affairs Program in the context of CS&C's overarching domestic cybersecurity mission.

NPPD developed a draft document, *DHS Implementation of the President's Strategy*, which highlights the key international engagements and programs that support the seven policy priorities outlined in the *Strategy*. As of December 2011, the document had not been finalized. In addition, although the QHSR and *Blueprint* drive the Department's cybersecurity mission and related international initiatives, neither defines how CS&C's and NCSD's international cybersecurity program goals will be achieved.

According to HSPD-7, DHS is responsible for developing a comprehensive plan outlining the goals and initiatives for protecting critical infrastructure, which includes a strategy for working with international organizations. In addition, the *Government Performance and Results Act Modernization Act of 2010* requires the development of a strategic implementation plan that identifies the major functions and operations of an agency. The plan should include general goals and objectives and a description of how those goals and objectives can be achieved. The strategic plan should cover at least 4 years following the fiscal year in which the plan is developed.

Constant management turnover has hindered CS&C's ability to develop a strategic implementation plan. For example, the following key personnel have departed NPPD within the past 10 months: the Deputy Undersecretary for NPPD in June 2011, the Director of US-CERT in July 2011, the Director of NCSD in January 2012, and the Assistant Secretary of CS&C in March 2012.

Without a strategic implementation plan, given the complexity of protecting cyberspace and constant leadership turnover within NPPD, it is difficult for CS&C to achieve its goals and objectives. It is crucial that a comprehensive implementation plan be developed to provide the necessary guidance and to allow CS&C to work with appropriate stakeholders to meet the requirements outlined in the *Strategy*.

Recommendation

We recommend that the Under Secretary, NPPD:

Recommendation #1:

Develop a comprehensive strategic implementation plan that defines CS&C's mission and priorities, specific roles and responsibilities, and detailed milestones for supporting the requirements outlined in the President's *Strategy*.

Management Comments and OIG Analysis

NPPD concurred with Recommendation 1. CS&C's cybersecurity mission, priorities, roles, and responsibilities result from a combination of statutory authorities, presidential directives, the Administration's *International Strategy for Cyberspace*, the *Quadrennial Homeland Security Review*, and the *Blueprint for a Secure Future: The Cybersecurity Strategy for the Homeland Security Enterprise.* These authorities and strategies necessitate that CS&C develop a strategic implementation plan for international engagement that clearly synthesizes and sets forth priorities in the context of multiple mission roles and requirements. This strategic plan will also need to reflect CS&C's international activities related to its communications missions. The detailed milestones included in any implementation plan will need to account for interagency and international decision-making processes over which CS&C has little control and which may lengthen completion timelines due to unforeseen circumstances.

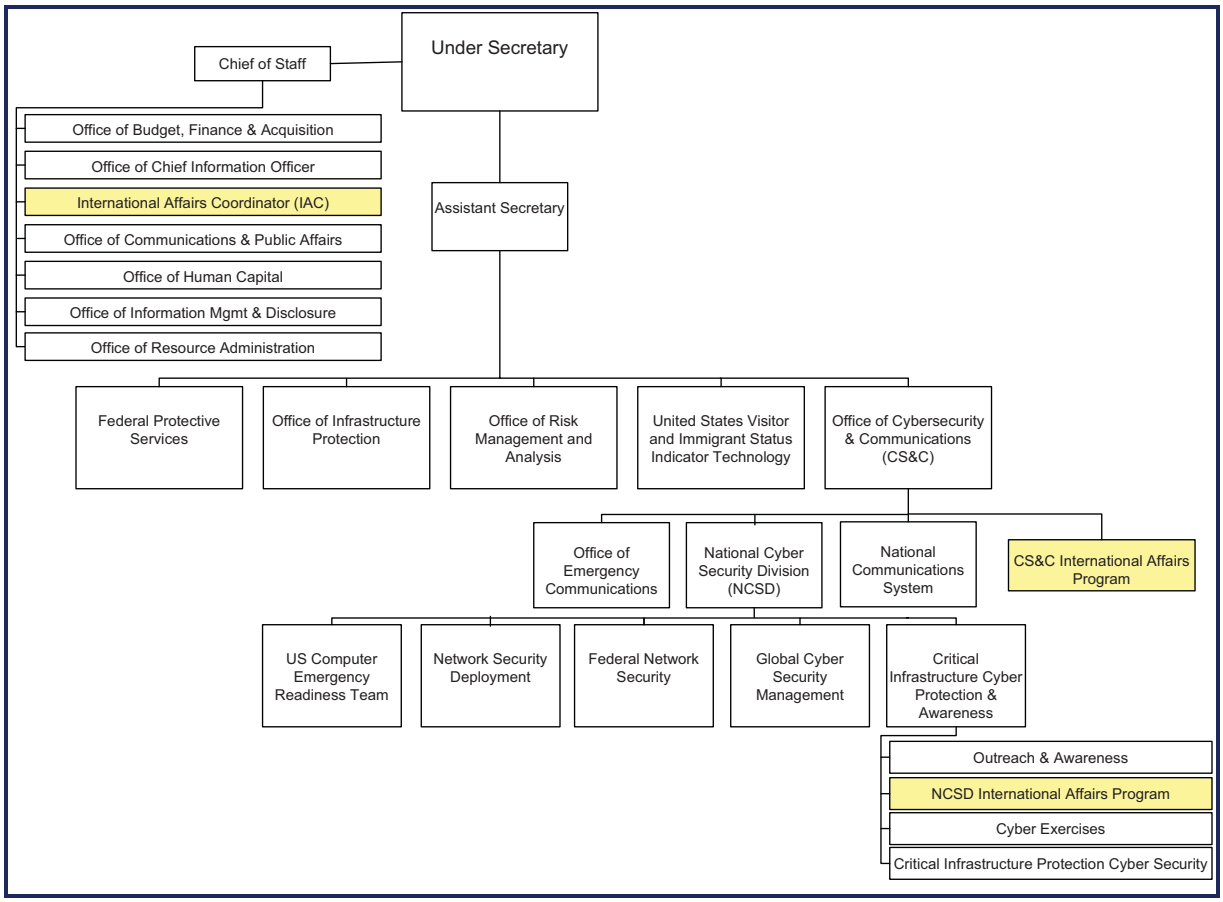
OIG Analysis

We agree with management's response to satisfy this recommendation. This recommendation will remain open until CS&C provides documentation to support that the planned corrective action is completed.

Streamlining NPPD's International Affairs Program and Processes Can Improve Efficiency

NPPD has not streamlined its International Affairs Program and processes to efficiently support its international cybersecurity goals, objectives, and priorities. For example, as of March 2012, NPPD had multiple international affairs functions operating at different directorate levels. Within the Office of the Under Secretary, the International Affairs Coordination function serves as the overarching program responsible for planning, prioritizing, and coordinating international engagements across NPPD. The International Affairs Coordination Program is also responsible for developing and implementing a Directorate-wide strategic framework for international engagements. In addition to NPPD International Affairs Coordination, international affairs programs are operating at the CS&C and NCSD levels. Figure 3 identifies the international affairs programs included in our review.

Figure 3: NPPD Organization Chart



Source: DHS OIG.

Since 2007, several organizational changes and additions have led to the creation of multiple international affairs programs within NPPD. According to the International Affairs Coordination Program's Acting Director, each international affairs program office manages its own engagements. Further, communication and coordination between the International Affairs Coordination Program and CS&C's and NCSD's international programs has been limited, resulting in travel inefficiencies and duplication of efforts.

To improve communication and collaboration and better leverage resources, the International Affairs Coordination Program drafted a proposal to centralize NPPD's international affairs functions into a single program.[5] The proposal,

[5] The proposal to centralize NPPD's international affairs functions includes not only those within CS&C, but also those within the Office of Infrastructure Protection and the United States Visitor Immigration Status Indicator Technology.

which is under review, was developed to drive strategy, improve coordination and transparency, and realign resources among each of the NPPD international affairs program functions. NPPD management is also exploring other proposals for improving the efficiency and effectiveness of NPPD's international affairs functions. These proposals offer different options for potential structural and process improvements.

The Office of Management and Budget's Circular A-123, Revised, requires Federal agencies to take systematic and proactive measures to develop and implement appropriate, cost effective internal controls for results oriented management. Specifically, agencies are responsible for implementing internal controls to achieve effective and efficient operations.

Until NPPD streamlines its international affairs activities and processes, the Directorate will not operate as efficiently and effectively as possible. As a result, NPPD may not be able to effectively support its international cybersecurity goals, objectives, and priorities until steps are taken to streamline and realign its respective international affairs resources and processes.

Recommendation

We recommend that the Under Secretary, NPPD:

Recommendation #2:

Take steps to streamline NPPD's international affairs activities and processes to improve transparency and reduce inefficiencies while supporting NPPD's international engagements.

Management Comments and OIG Analysis

NPPD concurred with Recommendation 2. NPPD is continuing its internal review process already underway, which the OIG references in the report, and which is expressly designed to evaluate all possible solutions, and combinations thereof, to improve the conduct of NPPD's international programs. NPPD continues to maintain an open line of communication with its subcomponents to alleviate any duplicated efforts. NPPD recognizes the need to complete its review in an expeditious manner. Therefore, while solutions are identified, NPPD is taking immediate action. An example of NPPD's process improvement is the rollout of a Directorate-wide international affairs prioritization and strategic planning process that will help ensure all elements of NPPD's international affairs

activities, regardless of where they are located within the organization, are conducted in accordance with U.S. Government, Department, and Directorate goals and objectives and have clearly identified expected outcomes. The new prioritization and strategic planning process is a good example of the type of substantitive improvements that will be part of the suite of solutions necessary to achieve the goal established in the OIG's recommendation.

While NPPD concurs with this recommendation, NPPD reiterates that the organizational chart included in the report to demonstrate the international programmatic organizational structure highlights only the existing international affairs program and does not reflect the international work that occurs across the organization. International engagement is supported by many programs and activities.

OIG Analysis

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until NPPD provides documentation to support that corrective action is completed.

US-CERT Can Improve Communication to Foster and Support Trusted Relationships

US-CERT has made progress in improving communications, coordinating, and collaborating with foreign nations to improve cyber information sharing and build capacity. For example, between March and December 2011, US-CERT held or participated in more than 50 events with foreign nations, including bilateral meetings, cyber exercises, international forums, and facility tours.

Still, US-CERT is not consistently communicating or developing personal relationships with all of its international counterparts, which has restricted its ability to develop trust based relationships required to share and receive actionable cyber threat information. It needs to take additional steps to enhance its relationships with the international community to strengthen cybersecurity.

From October 2011 to February 2012, we gathered information from seven international computer emergency response teams (CERTs) and cyber incident response centers to evaluate their levels of coordination, communication, and

collaboration with US-CERT regarding international cybersecurity.[6] Although many of the international CERTs we contacted acknowledged that US-CERT has established effective programs and technologies to collaborate and share information with the international community regularly, they also identified a number of improvements that can be made to develop stronger, trust based relationships. For example, two international CERTs indicated that US-CERT has not responded timely to their submissions on the [redacted].

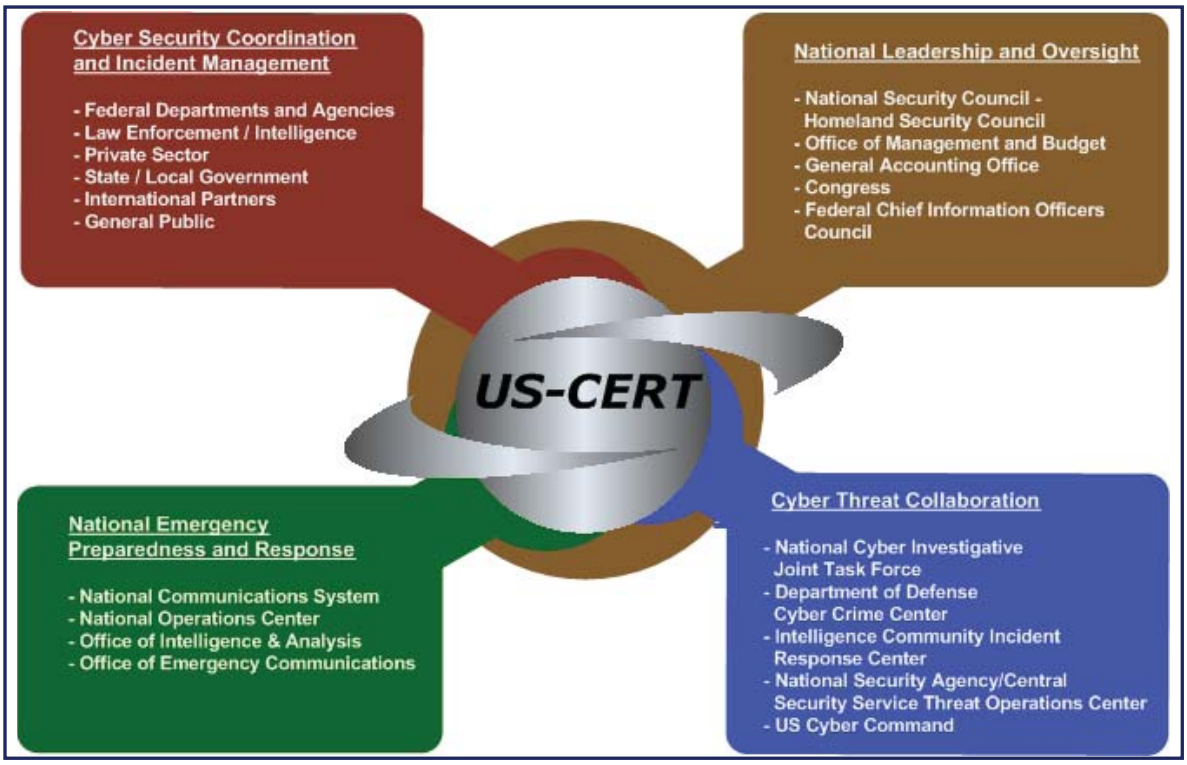
In addition, international CERTs have described their communication with US-CERT as one-directional. Specifically, the international CERTs indicated that even though they are providing information to US-CERT, US-CERT is not providing the desired feedback in response. Three of the CERTs we surveyed indicated that US-CERT has not provided direct points of contact to maintain an open dialogue and develop a "hands-on" relationship. Some of the international CERTs we visited also stated that US-CERT has not directly contacted them or taken the time to develop personal relationships with their personnel. For example, one international CERT said that it had never been contacted by US-CERT to discuss cyber threats or share best practices.

Because of staffing shortages and commitments to its primary mission areas, US-CERT has not dedicated specific staff to oversee or manage its international relationships on a regular basis. According to US-CERT, if additional staffing resources were made available, they could foster better relationships with international CERTs. This might include participating in more regional events, reviewing and following up on its cyber report distributions, and organizing additional international CERT site visits. In the draft *DHS Implementation of the President's Strategy*, the Department acknowledged the need for additional human resources to support international engagements and meet the United States' cybersecurity and foreign policy objectives.

Figure 4 illustrates US-CERT's operating environment, which aims to initiate two-way exchanges in order to collect incident information that may affect the Nation's cyber infrastructure.

[6] We collected data from cyber response teams in Canada, Denmark, Finland, [redacted] Norway, Qatar, and the United Kingdom.

Figure 4: US-CERT's Operating Environment



Source: US-CERT.

The *Strategy* recommends that the United States provide knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity. In addition, the United States should continue to develop and regularly share international cybersecurity best practices with its international partners. Further, the *DHS International Strategic Framework* requires the Department to build internal communication and coordination mechanisms to ensure that it promotes the development of a global security environment and adequately and appropriately responds to foreign government requests for partnership and assistance.

The nature of international relationships is such that, without improved communication, some international CERTs and counterparts may be reluctant to maintain a strong, trust-based working relationship with US-CERT. Establishing regular communication and personal dialogue with its international counterparts will allow US-CERT to build capacity with other countries and take steps to secure cyberspace collectively.

Recommendations

We recommend that the Under Secretary, NPPD:

Recommendation #3:

Ensure that sufficient US-CERT resources are dedicated to maintaining and actively pursuing new relationships with the international community.

Recommendation #4:

Develop and implement policies and procedures for establishing and maintaining open dialogues with foreign partners regarding cyber threats and vulnerabilities.

Management Comments and OIG Analysis

NPPD concurred with Recommendation 3. NPPD recognizes the importance of tactical information sharing and operational collaboration at the CERT-to-CERT level, and NPPD has already dedicated significant resources to physical and cybersecurity international engagement. US-CERT continues to build organizational international relationships based on defined, sustainable processes and operational requirements, and it synthesizes information across stakeholder communities. In the context of US-CERT's primary cybersecurity mission, NPPD believes that US-CERT already dedicates sufficient resources and attention to the international community.

The OIG found that US-CERT does not consistently communicate or develop personal relationships with all of its international counterparts. However, US-CERT focuses on building trust relationships between organizations—which are less likely to deteriorate with staffing changes—rather than focusing on personal relationships that develop on a case-by-case basis. NPPD is unclear as to why this is not an appropriate approach and what criteria the OIG utilized to evaluate relationship building.

Beyond the findings set forth in the OIG report, resources also are dedicated to operational international engagement by the Industrial Control Systems Cyber Emergency Response Team and the National Cybersecurity and Communications Integration Center. Furthermore, the Research and Standards Integration Program, the Cybersecurity Exercise Program, and the CS&C International Affairs function all regularly dedicate resources to support operational international

engagement with a range of international partners and are supported by other programs as required.

OIG Analysis

Though NPPD believes that US-CERT already dedicates sufficient resources and attention to the international community, this belief was not expressed during our discussions with the international CERT personnel included in our audit. International CERT personnel expressed concerns regarding not knowing who to contact at US-CERT, and US-CERT's responsiveness to calls for discussion or information. The OIG is not evaluating or recommending any specific type of relationship building with foreign counterparts, but simply presenting the information that we obtained from international CERT personnel. Although we agree that US-CERT's primary mission is not to collaborate with the international community, US-CERT needs to maintain and continually build upon relationships with its foreign counterparts to improve cybersecurity. This collaboration is necessary in light of high profile global cyber attacks. This recommendation will remain open until NPPD provides documentation to support that corrective action will be taken.

NPPD concurred with Recommendation 4. The Administration's *International Strategy for Cyberspace* highlights the need for information sharing in "an interconnected global environment." Open dialogue with foreign partners regarding cyber threats and vulnerabilities mutually benefits NPPD, foreign partners, and their respective stakeholders and customers. NPPD will examine its current internal policies and procedures related to such dialogue and address any identified gaps. NPPD currently has relationships with many countries that guide operational information sharing. However, it is important to note that the Federal Government has established information sharing policies that NPPD must follow. In particular, data sensitivity issues, foreign disclosure requirements, and privacy concerns present barriers that require the development and implementation of policies and procedures not only by DHS, but also U.S. public and private sector organizations, foreign counties, and international organizations.

OIG Analysis

We agree that the action being taken satisfies the intent of this recommendation. This recommendation will remain open until NPPD provides documentation to support that corrective action is completed.

Information Sharing Capabilities Could Be Strengthened to Enhance NPPD's International Relationships and Partnerships

NPPD and CS&C have not developed an information sharing policy to allow the free exchange of cyber data with other nations. In addition, information sharing with foreign partners has been hindered because of varying classification policies, privacy concerns, and cultural barriers. As a result, the information exchanged between NPPD, its foreign partners, and the international community may not be actionable, as the information sometimes is not timely or does not contain sufficient detail to address specific cyber threats.

NPPD has yet to develop specific international information sharing policies to identify the type of information that can be shared and countries with which it can be shared. Currently, CS&C's and NCSD's international affairs programs share unclassified and publicly available information regularly with their international partners. To facilitate information sharing, CS&C and NCSD rely on US-CERT's standard operating procedures and have implemented the internationally recognized standard, known as the Traffic Light Protocol.[7] In addition, NCSD utilizes formalized agreements established by DHS and other Federal agencies to share cyber threat information with its international partners. Classified information must be cleared by the Department's Foreign Disclosure Office before being shared with foreign nations.

Owing to the restrictions on classified information and privacy concerns, sensitive cyber incident data is not shared freely with international CERTs. For example, one international CERT said that it would like US-CERT to share specific cyber threat data, such as threat signatures. However, US-CERT personnel said that such data is proprietary information and cannot be shared because of national security concerns. In addition, US-CERT has indicated that some countries are not willing to provide specific incident data owing to their own privacy laws or restrictions. General information is typically shared.

The [redacted], as well as US-CERT's public website, are US-CERT's primary means of providing cybersecurity data (i.e., cyber threat warning information) to its international counterparts.[8] As part of its information sharing program, US-CERT also disseminates cyber threat information based on the Traffic Light Protocol. However, [redacted]

[7] The Traffic Light Protocol is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).
[8] http://www.us-cert.gov/.

[redacted] have approved the use of the Traffic Light Protocol. [redacted] receive only the general technical warning advisories and bulletins that are posted on US-CERT's public website.

In addition, foreign governments have developed their own policies for classifying sensitive information. As a result, sensitive data is being classified inconsistently among different countries, which prevents US-CERT from sharing cyber threat information with international CERTs. One of the CERTs we surveyed indicated that the inconsistent classification requirements hinder foreign countries' abilities to share cyber threat data timely, as information shared must be approved by different authorities in various countries before it can be disseminated to international partners and private organizations.

Further, cultural differences have limited the amount and quality of cyber threat information that international CERTs are willing to share with US-CERT. For example, some foreign partners are reluctant to share cyber threat data directly with US-CERT; instead, they work with their more trusted foreign country partners, especially those with similar cultures or languages. Language barriers also compound this issue, as some countries find it difficult to translate cybersecurity information into English for US-CERT personnel. One international CERT expressed the need for US-CERT personnel to become proficient in other languages to improve information sharing.

The President's *Cyberspace Policy Review* recommends that the United States work actively with all countries to develop a trusted, safe, and secure cyber infrastructure that enables prosperity for all nations. Further, the *Blueprint* requires that the homeland security enterprise, including the Department, implement collaboration principles that will foster the transfer of specific, actionable cybersecurity information using approved methods, while protecting and ensuring privacy protection. Robust interaction among all levels of government, the private sector, and our international partners will enhance measures taken and decisions made to improve and protect cyberspace.

Without an information sharing policy, it will be difficult for NPPD and CS&C to exchange cyber data with foreign nations. In addition, the lack of an internationally recognized classification system prevents detailed cyber threat information from being shared with foreign nations and partners. Further, sensitive information that is needed to prevent or mitigate cyber risks and incidents may become ineffective if it is not provided timely. Finally, without continued engagement and commitment to address cultural differences,

US-CERT faces increased risk that cyber threat information sharing with its foreign partners will be inadequate and severely limited.

Recommendation

We recommend that the Under Secretary, NPPD:

Recommendation #5:

Conduct information sharing assessments to identify internal gaps and impediments in order to increase situational awareness and enhance collaboration with foreign nations.

Management Comments and OIG Analysis

NPPD concurred with Recommendation 5. NPPD intends to conduct information sharing assessments and develop its own operational policies and procedures to overcome information sharing impediments over which NPPD has control. NPPD currently has relationships with many countries that guide current information sharing. However, the Federal Government has established information sharing policies that NPPD must follow. In particular, data sensitivity issues, foreign disclosure requirements, and privacy concerns present barriers that require the development and implementation of policies and procedures not only by DHS, but also by U.S. public and private sector organizations, foreign countries, and international organizations.

OIG Analysis

We agree with management's response to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that the planned corrective action is 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 evaluate whether DHS, through NPPD's CS&C, has established effective programs and partnerships to collaborate and share cybersecurity information with the international community in order to promote the benefits of networked technology globally and a secure, reliable, and interoperable cyberspace. Specifically, we determined whether CS&C (1) has established policies and procedures to build upon and create new relationships to facilitate collaboration with international partners; (2) is taking steps to strengthen operational collaboration with its international counterparts to reduce cyber vulnerabilities and improve incident response and information sharing capabilities; and (3) is working with the international community and industry to share its expertise and goals regarding cybersecurity.

Our audit focused on the actions and recommendations, requirements, and goals outlined in *The National Strategy to Secure Cyberspace, International Strategy for Cyber Space, Cyberspace Policy Review, Quadrennial Homeland Security Review*, Homeland Security Presidential Directive – 7, and *Blueprint for a Secure Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, as well as other applicable guidance. To evaluate whether CS&C is coordinating its international activities, we interviewed selected officials within NPPD, including CS&C and NCSD personnel, as well as an industry representative and a Federal Agency official.

We also determined whether CS&C's policies and procedures comply with applicable cybersecurity guidance and promote collaboration with the international community. We observed bilateral and multilateral meetings and events, including the 2011 Meridian Conference, to assess CS&C's collaborative efforts. Furthermore, we conducted site visits with and surveyed seven international CERTs to determine whether US-CERT is sharing cyber threat information, incident response procedures, and other best practices.

Fieldwork was performed in Arlington, Virginia, and at selected locations in Denmark, Finland, [redacted], Norway, and Qatar. We conducted this performance audit between September 2011 and March 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.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

JUN 29 2012

Mr. Charles K. Edwards
Acting 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 Can Strengthen Its International Cybersecurity Programs* (OIG Project No. 11-149-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's (OIG) work in planning and conducting its review and issuing this report.

The Department is pleased to note the OIG has recognized the actions the National Protection and Programs Directorate (NPPD) and its subcomponents have taken to promote collaboration and develop partnerships with the international community. Several activities and international meetings are highlighted in the report, including operational information sharing by the United States Computer Emergency Readiness Team (US-CERT) and various international cybersecurity exercises developed, conducted, or otherwise engaged in by NPPD's Office of Cybersecurity and Communications (CS&C).

However, NPPD/CS&C is concerned that the report does not provide sufficient context for readers to fully appreciate NPPD's international cybersecurity mission and activities. For example, the report does not outline the significant roles of other Federal agencies in implementing the *International Strategy for Cyberspace*. While the OIG is only responsible for evaluating the role of DHS components, NPPD's activities are best understood in the context of the overall interagency effort. In addition, NPPD activities cited in the report are not fully representative of the breadth of NPPD's international cybersecurity initiatives. For example, CS&C contributes to international cybersecurity policy development as part of a broader U.S. Government effort. Officials within CS&C's Research and Standards Integration Program and the Software Assurance Program participate in international standards bodies to drive the adoption of cybersecurity standards that benefit the United States and its international partners. Similarly, the Control Systems Security Program collaborates with foreign countries and international organizations to improve the security of industrial control systems. The program offers training to domestic and international partners and provides advanced vulnerability analysis for domestic and international owners, operators, and vendors of industrial control systems. Additionally, the program's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) regularly shares operational security information with international partners.

Further, the NPPD organization chart that is included in the draft report to demonstrate the international programmatic organizational structure highlights the existing international affairs programs, but it does not fully reflect the international work that occurs across the organization.

NPPD/CS&C is concerned that the OIG's report could lead readers to assume that CS&C's primary mission is international cybersecurity cooperation. International collaboration is important and foreign engagement is necessary, but CS&C's authorities, roles, and responsibilities clearly establish international engagement as a supporting element of its overall cybersecurity mission. For example, the OIG correctly observes that Homeland Security Presidential Directive-7 (HSPD-7) requires DHS to develop "a comprehensive plan outlining the goals and initiatives for protecting critical infrastructure, which includes a strategy for working with international organizations." The National Infrastructure Protection Plan (NIPP) constitutes the comprehensive plan required by HSPD-7 and Section 4.1.4 of the NIPP is the associated strategy for working with international organizations. The NIPP further explains that DHS works with other Federal agencies and international partners "to exchange experiences, share information, and develop a cooperative environment *to materially improve U.S. [critical infrastructure] protection*" (emphasis added). This overarching context is not conveyed by the OIG report.

Beyond contextual matters, NPPD does have some sensitivity concerns and they, along with technical and accuracy comments, have been provided under separate cover. NPPD wants to ensure that these comments, particularly those that relate to diplomatic and operational security concerns, are addressed before the OIG issues the final report. We believe addressing these concerns warrants editing the existing draft report. It is our understanding that these issues will be separately addressed through further dialogue with your office.

Following are our detailed responses to the five recommendations made in the draft report.

Recommendation 1: Develop a comprehensive strategic implementation plan that defines CS&C's mission and priorities, specific roles and responsibilities, and detailed milestones for supporting the requirements outlined in the President's Strategy.

Response: Concur. CS&C's cybersecurity mission, priorities, roles, and responsibilities result from a combination of statutory authorities, presidential directives, the Administration's *International Strategy for Cyberspace*, the *Quadrennial Homeland Security Review*, and the *Blueprint for a Secure Future: The Cybersecurity Strategy for the Homeland Security Enterprise*. These authorities and strategies necessitate that CS&C develop a strategic implementation plan for international engagement that clearly synthesizes and sets forth priorities in the context of multiple mission roles and requirements. This strategic plan will also need to reflect CS&C's international activities related to its communications missions. The detailed milestones included in any implementation plan will need to account for interagency and international decisionmaking processes over which CS&C has little control and which may lengthen completion timelines due to unforeseen circumstances.

Recommendation 2: Take steps to streamline NPPD's international affairs activities and processes to improve transparency and reduce inefficiencies while supporting NPPD's international engagements.

Response: Concur. NPPD is continuing its internal review process already underway, which the OIG references in the report, and which is expressly designed to evaluate all possible solutions, and combinations thereof, to improve the conduct of NPPD's international programs. NPPD continues to maintain an open line of communication with its subcomponents to alleviate any duplicated efforts. NPPD recognizes the need to complete its review in an expeditious manner. Therefore, while solutions are identified, NPPD is taking immediate action. An example of NPPD's process improvement is the rollout of a Directorate-wide international affairs prioritization and strategic planning process that will help ensure all elements of NPPD's international affairs activities, regardless of where they are located within the organization, are conducted in accordance with U.S. Government, Department, and Directorate goals and objectives and have clearly identified expected outcomes. The new prioritization and strategic planning process is a good example of the type of substantive improvements that will be part of the suite of solutions necessary to achieve the goal established in the OIG's recommendation.

While NPPD concurs with this recommendation, NPPD reiterates that the organization chart included in the report to demonstrate the international programmatic organizational structure highlights only the existing international affairs programs and does not reflect the international work that occurs across the organization. International engagement is supported by many programs and activities.

Recommendation 3: Ensure that sufficient US-CERT resources are dedicated to maintaining and actively pursuing new relationships with the international community.

Response: Concur. NPPD recognizes the importance of tactical information sharing and operational collaboration at the CERT-to-CERT level, and NPPD has already dedicated significant resources to physical and cybersecurity international engagement. US-CERT continues to build organizational international relationships based on defined, sustainable processes and operational requirements, and it synthesizes information across stakeholder communities. In the context of US-CERT's primary cybersecurity mission, NPPD believes that US-CERT already dedicates sufficient resources and attention to the international community.

The OIG found that US-CERT does not consistently communicate or develop personal relationships with all of its international counterparts. However, US-CERT focuses on building trust relationships between organizations—which are less likely to deteriorate with staffing changes—rather than focusing on personal relationships that develop on a case-by-case basis. NPPD is unclear as to why this is not an appropriate approach and what criteria the OIG utilized to evaluate relationship building.

Beyond the findings set forth in the OIG report, resources also are dedicated to operational international engagement by the Industrial Control Systems Cyber Emergency Response Team and the National Cybersecurity and Communications Integration Center. Furthermore, the Research and Standards Integration Program, the Cybersecurity Exercise Program, and the

CS&C International Affairs function all regularly dedicate resources to support operational international engagement with a range of international partners and are supported by other programs as required.

Recommendation 4: Develop and implement policies and procedures for establishing and maintaining open dialogues with foreign partners regarding cyber threats and vulnerabilities.

Response: Concur. The Administration's *International Strategy for Cyberspace* highlights the need for information sharing in "an interconnected global environment." Open dialogue with foreign partners regarding cyber threats and vulnerabilities mutually benefits NPPD, foreign partners, and their respective stakeholders and customers. NPPD will examine its current internal policies and procedures related to such dialogue and address any identified gaps. NPPD currently has relationships with many countries that guide operational information sharing. However, it is important to note that the Federal government has established information sharing policies that NPPD must follow. In particular, data sensitivity issues, foreign disclosure requirements, and privacy concerns present barriers that require the development and implementation of policies and procedures not only by DHS, but also by U.S. public and private sector organizations, foreign countries, and international organizations.

Recommendation 5: Conduct information sharing assessments to identify internal gaps and impediments in order to increase situational awareness and enhance collaboration with foreign nations.

Response: Concur. NPPD intends to conduct information sharing assessments and develop its own operational policies and procedures to overcome information sharing impediments over which NPPD has control. NPPD currently has relationships with many countries that guide current information sharing. However, the Federal government has established information sharing policies that NPPD must follow. In particular, data sensitivity issues, foreign disclosure requirements, and privacy concerns present barriers that require the development and implementation of policies and procedures not only by DHS, but also by U.S. public and private sector organizations, foreign countries, and international organizations.

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

Sincerely,

Rand Beers
Under Secretary

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Barbara Bartuska, IT Audit Manager
Aaron Zappone, Team Lead
Michael Kim, IT Auditor
Pachern Thapanawat, IT Auditor
Shannon Frenyea, 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
Chief Information Officer, DHS
Chief Information Security Officer, DHS
Chief Information Officer, NPPD
Director, Compliance and Oversight Program, DHS OCISO
Director, OIG/GAO Audit Liaison Office, NPPD
NPPD Audit Liaison
Chief Information Security Officer Audit Liaison, DHS
CS&C External Affairs Audit Liaison
Program Analyst/Audit Liaison, NCSD

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: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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